The State of Spam

A Monthly Report – September 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 theme of the Symantec State of Spam Report for September centers on recent attacks that prove that there is no missing link between malware and spam. Spammers have demonstrated that they are willing to go to great lengths to spread malicious attachments. During the month of August, Symantec categorized 27 percent of spam as "Internet" related or goods or services offered online. This represents a 9 percent increase since June 2008 and can be attributed to messages that contain links to malware. Other spam attacks that contain malicious attachments are also prevalent with attachment spam accounting for 10 percent of all spam in August 2008. Overall spam levels remain constant over the past month with spam accounting for 80 percent of email through August 2008. The September report comments on the trends associated with the following:

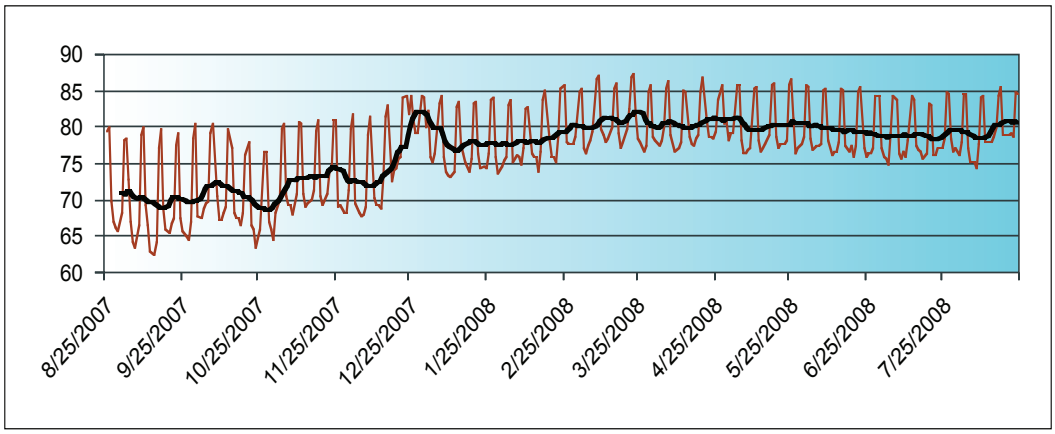
- **Breaking News...McCain Chooses Paris Hilton as Running Mate**
- **Russia/Georgia Conflict News Used to Hide Malicious Code in Spam**
- **Spammers Target Parents with Kidnapping Hoax**
- **Download IE7 ... the Latest Version**
- **Malware + Spam + Phishing = The Trifecta of Threats to Financial Institutions**
- **Job Seekers: Beware of Bogus Recruiting Ads bearing Viruses**
- **Delivery Company's Brand Packaged to Deliver Malware**
- **Airline E-ticket Connects Malicious Code and Spam**
- **Olympic-Themed Spam Continued in August 2008**

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



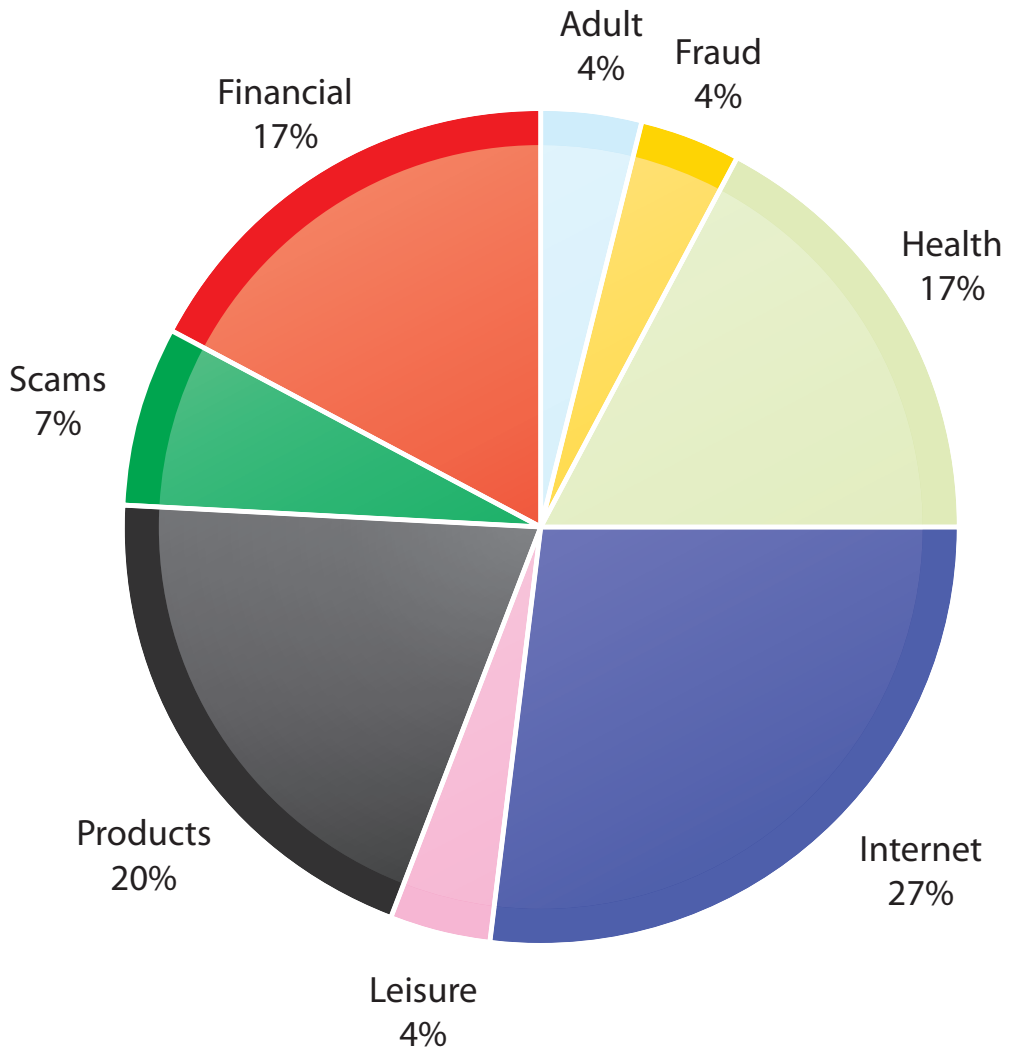
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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

Global Category Count 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*

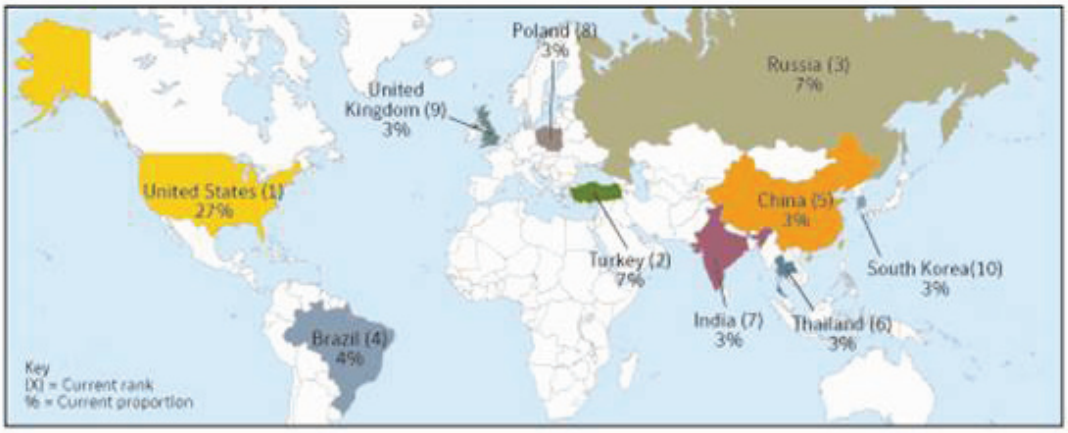
- **Spiritual E-mail attacks** with information pertaining to religious or spiritual evangelization and/or services. *Examples: psychics, astrology, organized religion, outreach*

- **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.



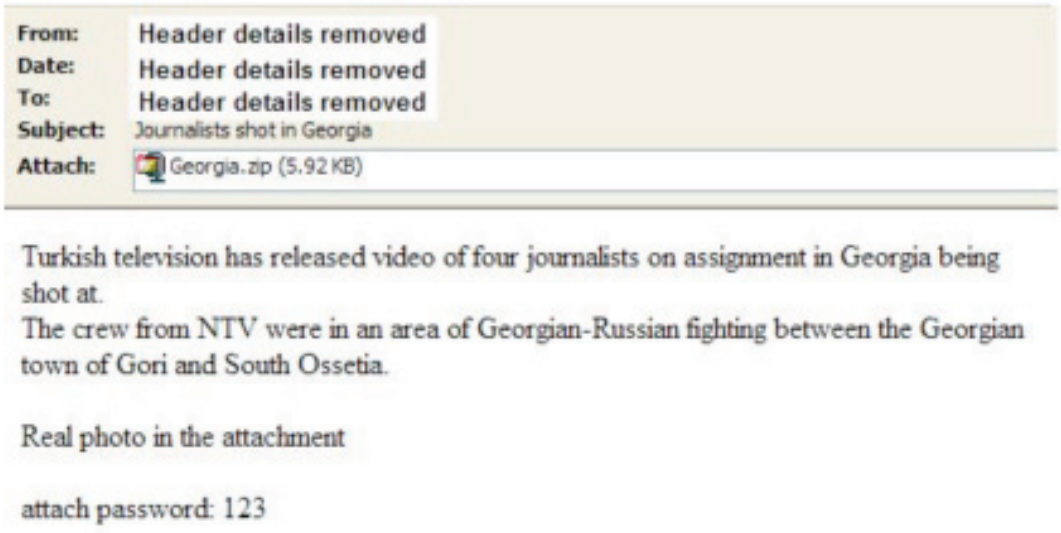
Breaking News...McCain Chooses Paris Hilton as Running Mate

Despite what spammers would like us to believe this is not breaking news. Statements like these were used regularly in spam messages during the month of August. These emails contain a link to malware designed to infect other computers with viruses and trojans rather than simply promoting a spam product. In June 2008 spam messages that fell into the Internet category stood at 18 percent of all spam messages. In August 2008 spam messages that fell into the Internet category stands at 27 percent. The 9 percent increase in the category of Internet spam since June 2008 can be attributed to the rise in spam messages that contain links to malware. Other spam attacks that contain malicious attachments are also prevalent with attachment spam averaging at 5 percent of all spam and reaching a maximum of 10 percent of all spam in the last 30 days. In the last month Symantec has observed various spam attacks illustrating that there are no missing links between malware and spam.

Russia/Georgia Conflict News Used to Hide Malicious Code in Spam

In August 2008, Symantec observed malware spam masquerading as news articles regarding the current Georgia-Russia conflict. As this particular event is garnering significant media attention there is a significant risk of the spreading of malicious code by spam email using information on this conflict as a lure. The messages contain an attachment, along with instructions and passwords to download the attachment. The subject line appears to be a legitimate news story about the Russia/Georgia conflict. One subject line that has been seen reads: "Subject: Journalists Shot in Georgia." A short description of the supposed event is contained within the body of the message.

The use of the attention-grabbing subject line seems to be intended as a social engineering tactic to entice recipients to click the link and view videos. The attachment does not contain a video, and instead redirects to a link that delivers a payload identified as Trojan.Popwin. Symantec offer protection to its customers against this malware.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Journalists shot in Georgia
Attach: Georgia.zip (5.92 KB)

Turkish television has released video of four journalists on assignment in Georgia being shot at.
The crew from NTV were in an area of Georgian-Russian fighting between the Georgian town of Gori and South Ossetia.

Real photo in the attachment

attach password: 123

Spammers Target Parents with Kidnapping Hoax

The avenues that spammers will explore to spread their malicious intentions seems to have no bounds. In the following example a spammer tries to convince an unsuspecting parent that they have kidnapped the recipient's child and that a ransom must be paid. The spammer indicates that they have attached a photo of the child as proof but instead offers malware in the attachment. In this example the spammer is trying to tug at the heart strings of parents to panic them into opening a malicious attachment.

Download IE7 ... The Latest Version
In August 2008, Symantec observed a very high profile attack that invited users to download a free version of Internet Explorer 7. The message contained a dotted quad URL with a .exe download. Dotted quad spam occurs when the dotted quad address of the spam URL link is used in the spam message body rather than the domain name of the spam URL. The .exe download was detected as tojan.bluesod. This attack is also closely related to a celebrity video download attack that has been prevalent in recent months. Antispam filters created against this attack have fired over 200 million messages in the last month.


From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Internet Explorer 7

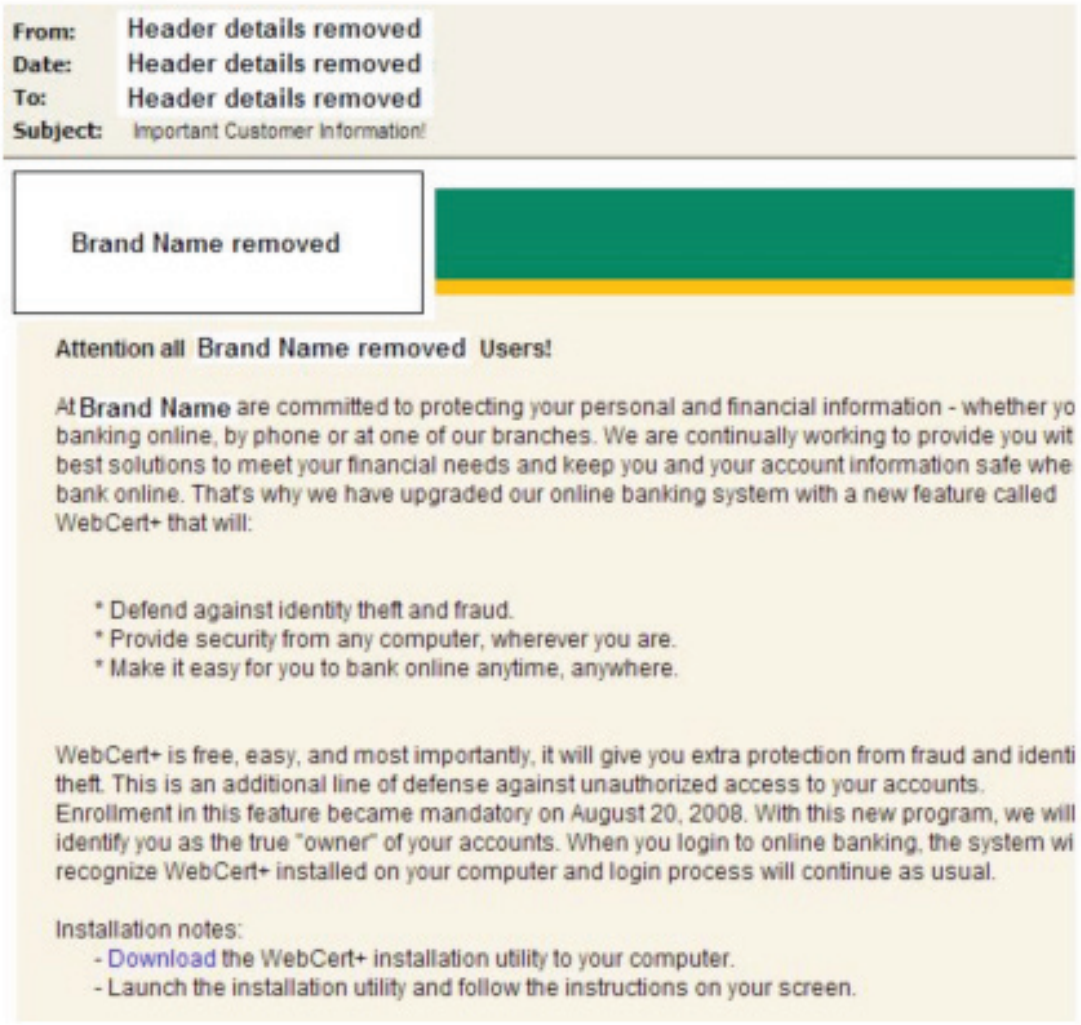
Download the latest version!

About this mailing:
You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive this MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

?2008 Microsoft | Unsubscribe | More Newsletters | Privacy

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Malware + Spam + Phishing = The Trifecta of Threats to Financial Institutions
A recent trifecta of security threats was observed in a spam attack observed by Symantec in August. One financial institution in particular was targeted. The spam message informed the recipient that the financial institution was introducing new security measures to protect against fraud and identity theft. The message indicates that the security measures are mandatory and the feature is been introduced immediately. The message notes that by downloading an attached program the customer will obtain protection. This is a different approach for spammers as they have typically asked recipients to update customer account details using a bogus URL link.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Important Customer Information!

Brand Name removed

Attention all Brand Name removed Users!

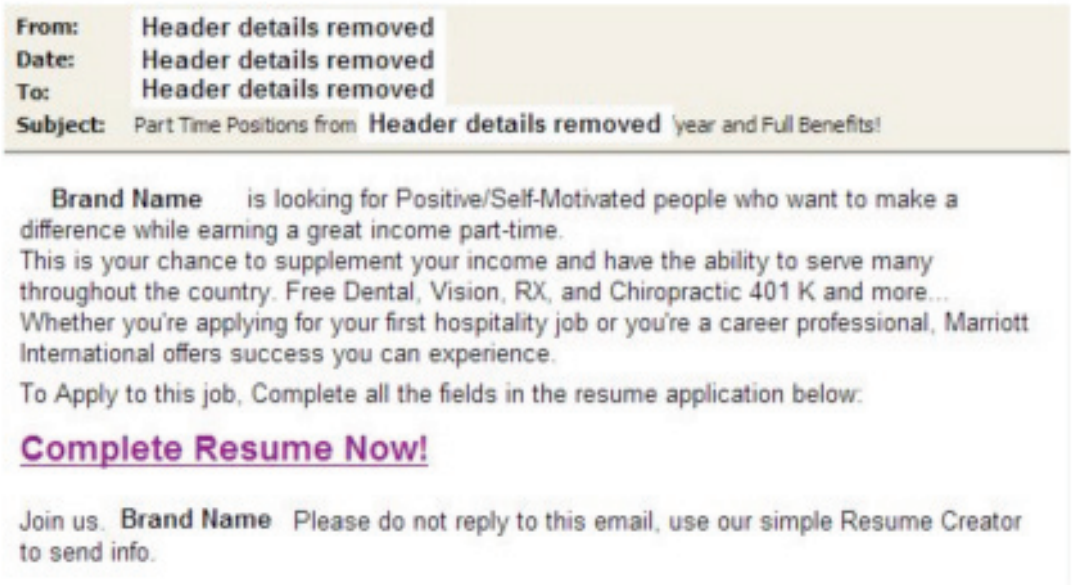
At Brand Name are committed to protecting your personal and financial information - whether yo banking online, by phone or at one of our branches. We are continually working to provide you wit best solutions to meet your financial needs and keep you and your account information safe whe bank online. That's why we have upgraded our online banking system with a new feature called WebCert+ that will:

* Defend against identity theft and fraud.
* Provide security from any computer, wherever you are.
* Make it easy for you to bank online anytime, anywhere.

WebCert+ is free, easy, and most importantly, it will give you extra protection from fraud and identi theft. This is an additional line of defense against unauthorized access to your accounts. Enrollment in this feature became mandatory on August 20, 2008. With this new program, we will identify you as the true "owner" of your accounts. When you login to online banking, the system wi recognize WebCert+ installed on your computer and login process will continue as usual.

Installation notes:
- Download the WebCert+ installation utility to your computer.
- Launch the installation utility and follow the instructions on your screen.

Job Seekers: Beware of Bogus Recruiting Ads bearing Viruses
The worst thing people expect to receive when they apply for a job is an automated message from an employer kindly informing them that their skills do not match those of the position advertised. In a recent spam attack a prospective employee could have received something far more sinister – malware. The message in question purported to come from an employer offering a part-time position where its compensation included many enticing benefits. However in order to apply for the position the prospective employee was instructed to click on a link with a .exe download.


From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Part Time Positions from Header details removed year and Full Benefits!

Brand Name is looking for Positive/Self-Motivated people who want to make a difference while earning a great income part-time.
This is your chance to supplement your income and have the ability to serve many throughout the country. Free Dental, Vision, RX, and Chiropractic 401 K and more...
Whether you're applying for your first hospitality job or you're a career professional, Marriott International offers success you can experience.
To Apply to this job, Complete all the fields in the resume application below:

Complete Resume Now!

Join us. Brand Name Please do not reply to this email, use our simple Resume Creator to send info.

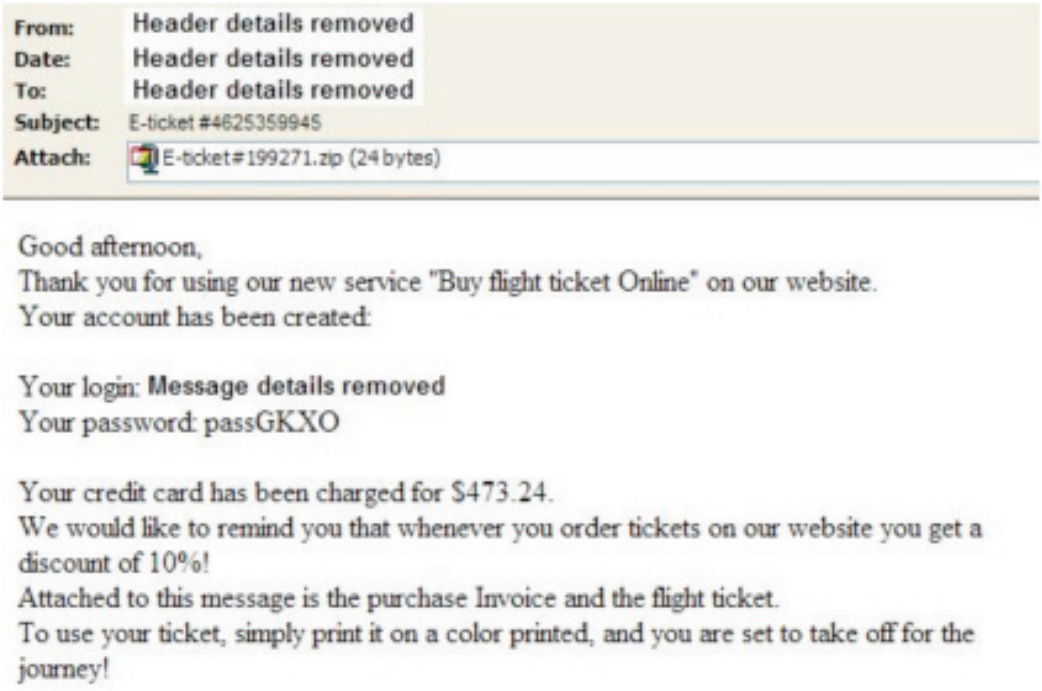
Delivery Company's Brand Packaged to Deliver Malware
Another example that proves that there is no missing link between malware and spam is an attack that uses a delivery company's brand. The message claims that the company is unable to deliver package because of an invalid address and that the sender needs to collect the parcel from the delivery company's office. However in order to claim the parcel the recipient is instructed to print a copy of the invoice which is attached to the message. The invoice however is a virus.


From: Header details removed
Date: Header details removed
To: Header details removed
Subject: TRACKING NUMBER 7532518473
Attach: Exel_Invoice_NR719200.zip (50.7 KB)

Unfortunately we were not able to deliver postal package you sent on August the 1st in time
because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office

Your Brand Name removed

Airline E-ticket Connects Malicious Code and Spam
Yet another instance which demonstrates the connection between malware and spam is a recent spam message that claimed to be an airline e-ticket. This attack thanked the recipient for using their online services “Buying flight ticket Online” and informed the user that the attached message is the purchase invoice and the flight ticket. The e-ticket invoice attachment which was in a .zip file format, results in the Trojan horse “Infostealer.Monstress” being executed. On August 16th this Trojan targeted millions of customer records uploaded on a recruitment web site.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: E-ticket #4625359945
Attach: E-ticket#199271.zip (24 bytes)

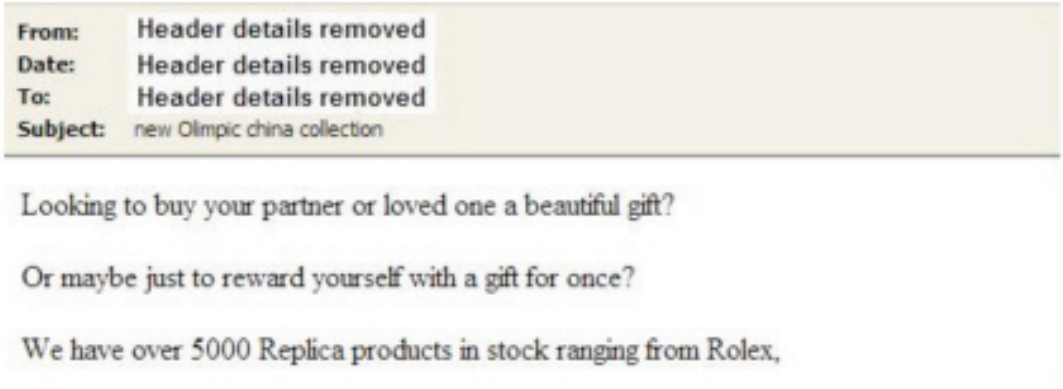
Good afternoon,
Thank you for using our new service "Buy flight ticket Online" on our website.
Your account has been created:

Your login: **Message details removed**
Your password: passGKXO

Your credit card has been charged for $473.24.
We would like to remind you that whenever you order tickets on our website you get a discount of 10%!
Attached to this message is the purchase Invoice and the flight ticket.
To use your ticket, simply print it on a color printed, and you are set to take off for the journey!

Olympic-Themed Spam Continued in August 2008

As the Olympic Games concluded in late August, Olympic-themed spam continued. References to the Olympic Games were used to promote a number of products such as watches and Chinese training spam. While the spam employed techniques such as message obfuscation and spam URLs inserted into the message body are not new, it did demonstrate spammers' willingness to join the games in their own unique way.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: new Olimpic china collection

Looking to buy your partner or loved one a beautiful gift?

Or maybe just to reward yourself with a gift for once?

We have over 5000 Replica products in stock ranging from Rolex,