The State of Spam

A Monthly Report – September 2007

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Monthly Spam Landscape

August was an interesting month for spam observers with overall spam activity increasing by 3% to just under 70% of all email traffic, PDF spam recording highs and lows, and YouTube making a malicious entrance similar to recent Ecard spam tactics.

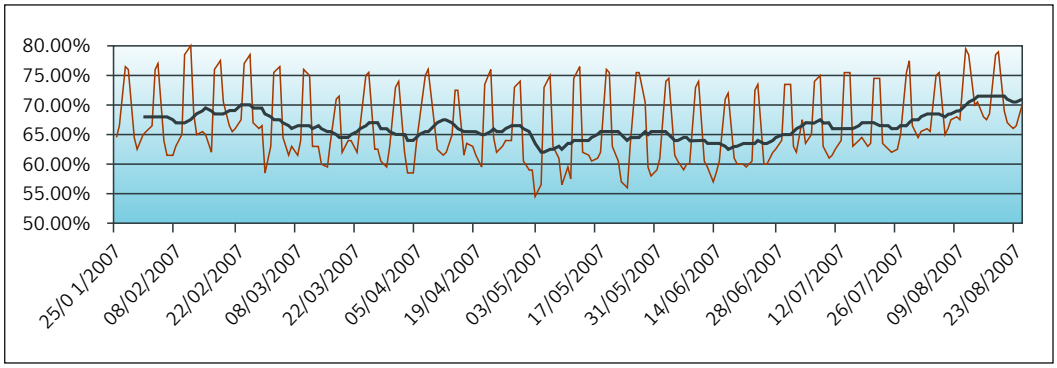
Highlights included:

- Spam Levels Inch Upwards. Overall spam levels at the SMTP layer in August increased averaging 69% of total email. This compared with 66% of total email in July. (See Page 1)
- From Ecards to YouTube – Spammers continue to blast out a variety of attacks containing malicious URLs. This type of attack accounted for up to 15% of all spam in August (see Page 7)
- PDF Spam, a Flash in the Pan? PDF and attachment spam proved to be August's flash in the pan. In early August, a dramatic increase in PDF spam was recorded, and at its peak, Symantec estimated that PDF spam accounted for nearly 20% of all spam. As August ended, a dramatic fall-off in PDF spam was recorded, accounting for less than 1% of all spam. (See Page 6)
- Image Spam Maintains Steady Appearance. No major changes in image spam levels were observed in August as it continued to hover around 10% of total spam. (See Page 5)
- Additional insight is provided below on the following tactics:
  - Update: Spam messages containing URLS with Chinese domains
  - 419 spam hasn't gone away
  - Join the police force spam
  - Chinese jigsaw training spam images
  - Novel puppy scam email

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.



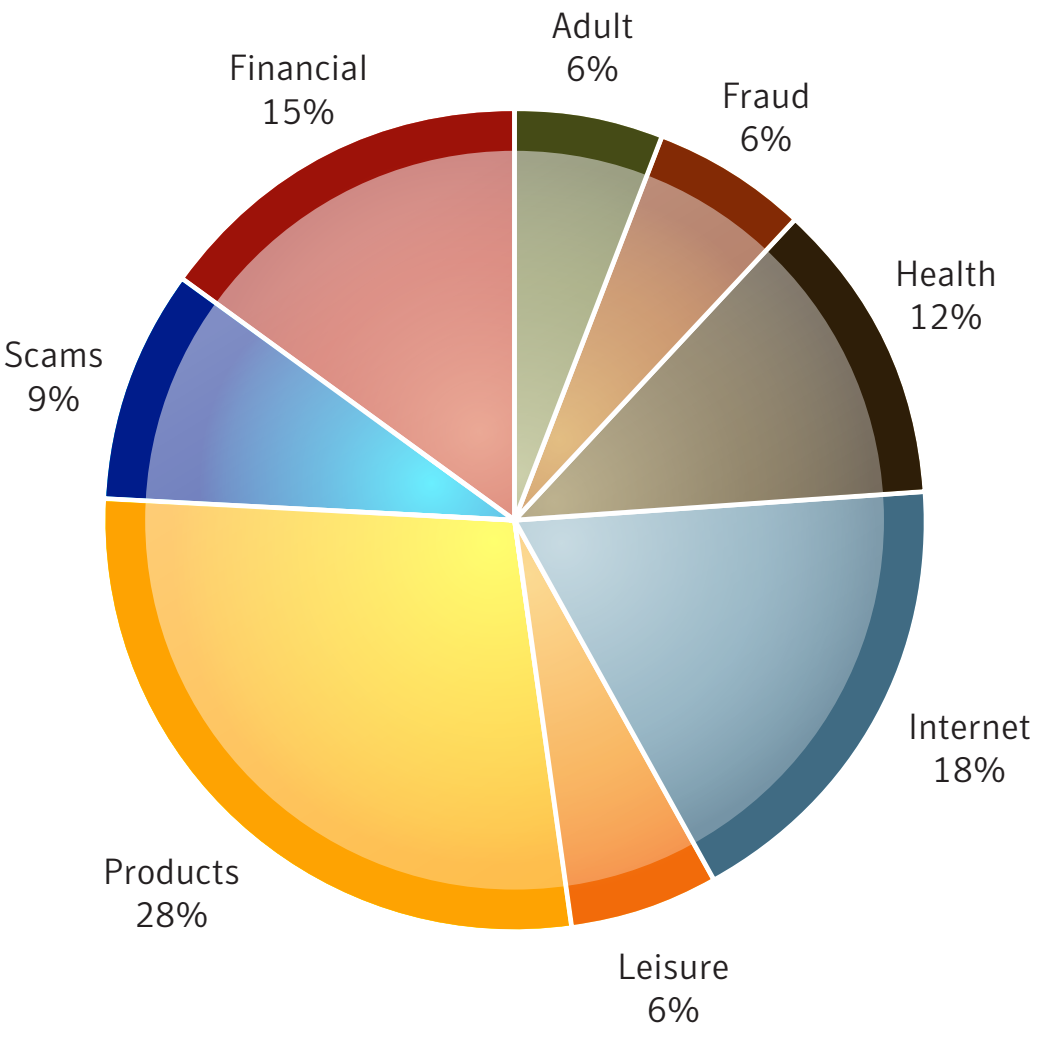
A trend line has been added to demonstrate a 7-day moving average.

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**

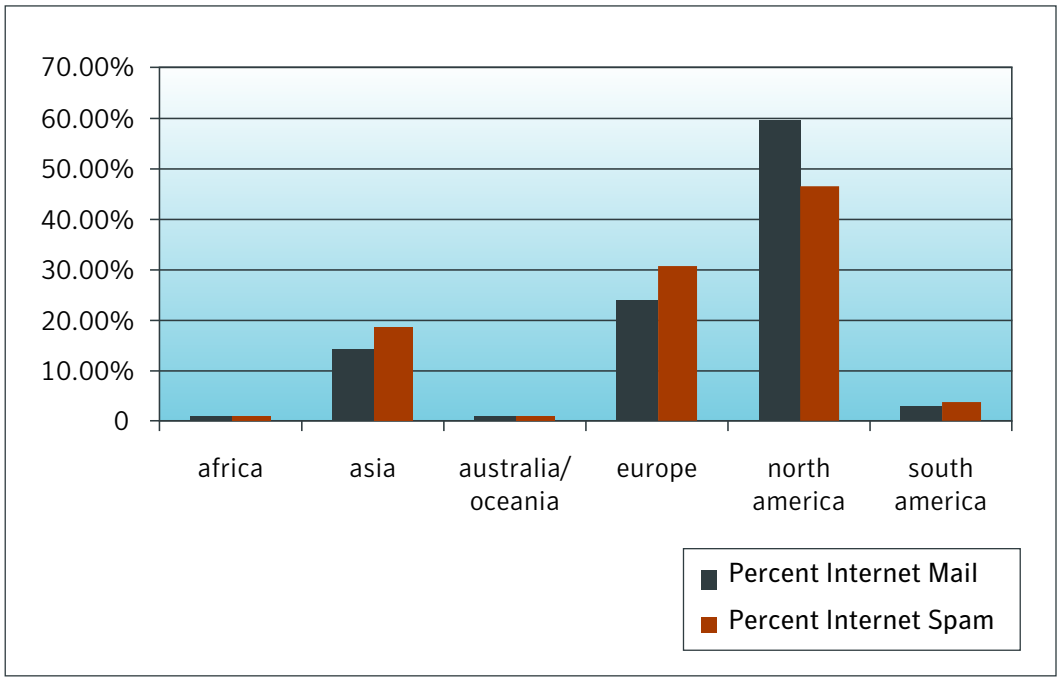
- **Other Emails attacks** not pertaining to any other category.

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.

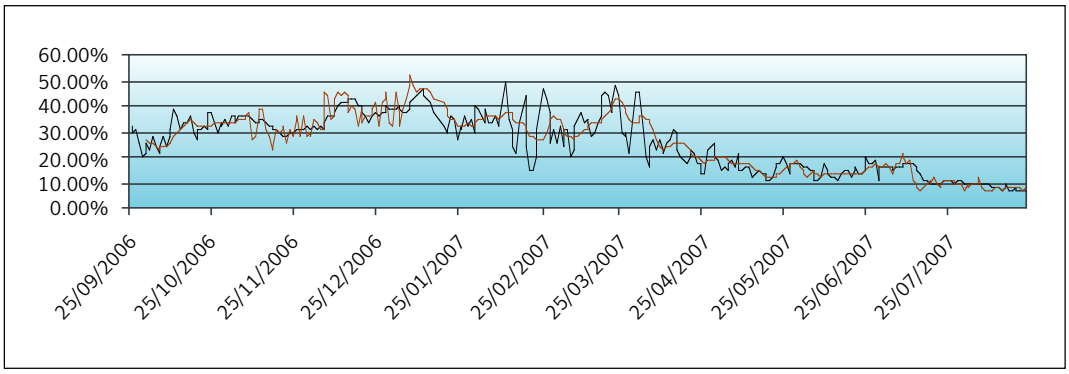
Global Claimed Region of Origin – Last 90 Days



Percent Image Spam

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

Internet Email – Percent Image Spam



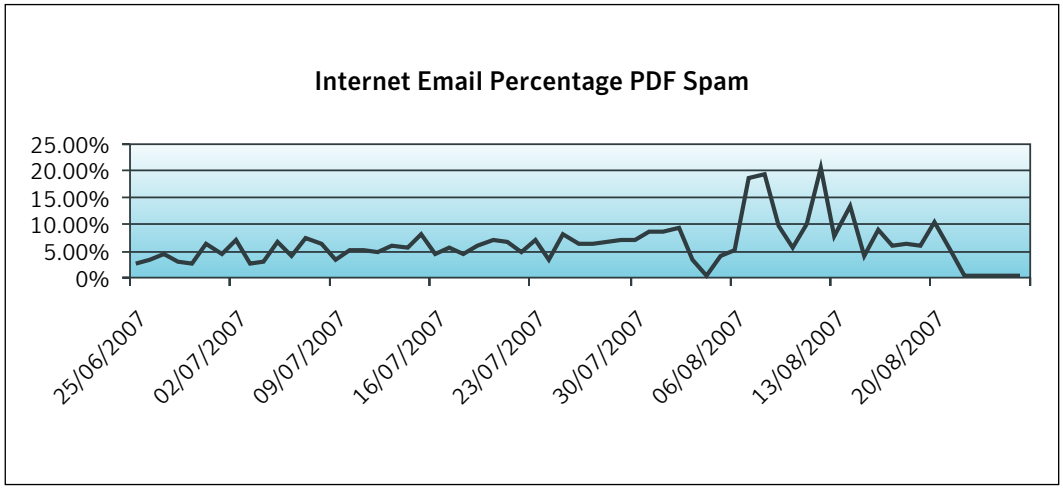
A trend line has been added to demonstrate a 7-day moving average.

Additional Insights

PDF Spam - a Flash in the Pan?

In June, Symantec observed the emergence of PDF and other attachment spam. August has been an interesting month for this type of spam. In early August, a dramatic rise in PDF spam was recorded, and at its peak, Symantec estimated that PDF spam accounted for nearly 20% of all spam. At its peak, PDF files continued to be the dominant mode of attachment spam, though other variants such as XLS and RAR files were also observed, albeit in smaller numbers.

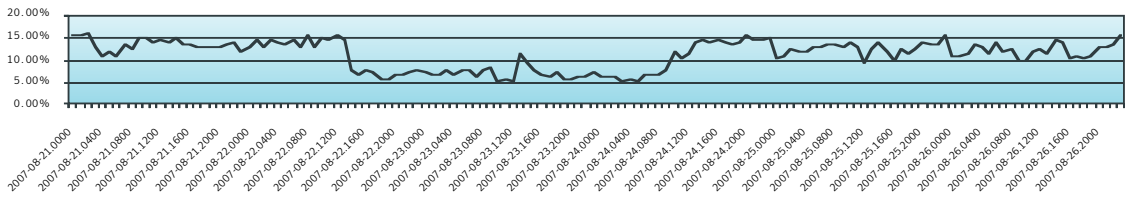
As the month of August progressed, a dramatic decline in PDF spam was observed closing out at less than 1% of total spam. This decline in PDF spam shows similarities with the decrease in image spam. Antispam vendors' success with blocking PDF spam to date illustrates how the lifespan of new spam attacks correlates with how much effort is required by spammers in order to circumvent antispam filters. While the future for this spam trend remains unclear, Symantec will continue to monitor this trend closely.



From Ecards to YouTube

Symantec reported in July that Ecard spam had become particularly virulent and August saw this trend continue. These attacks continue to morph and included different hooks intended to entice end users into following a malicious URL. One high profile example in August attempted to fool users into thinking they were going to watch a YouTube video.

A common characteristic of many of these attacks is the use of a "dotted quad URL":



The "dotted quad" numeric IP URL addresses contained in the messages send the uninformed to a malicious link hosting malware. The malware hosting URL is always an IP address and the large number of these URLs indicates the vast number of hosts available to the authors of this vulnerability. As this spam has evolved, so has the malware being propagated. The authors have added functionality to hide some of the infections and are constantly attempting to evade AV/IPS detections. This piece of malware is primarily detected by Symantec as Trojan.Packed.13 (TP.13) or as some variant of Trojan.Peacomm.

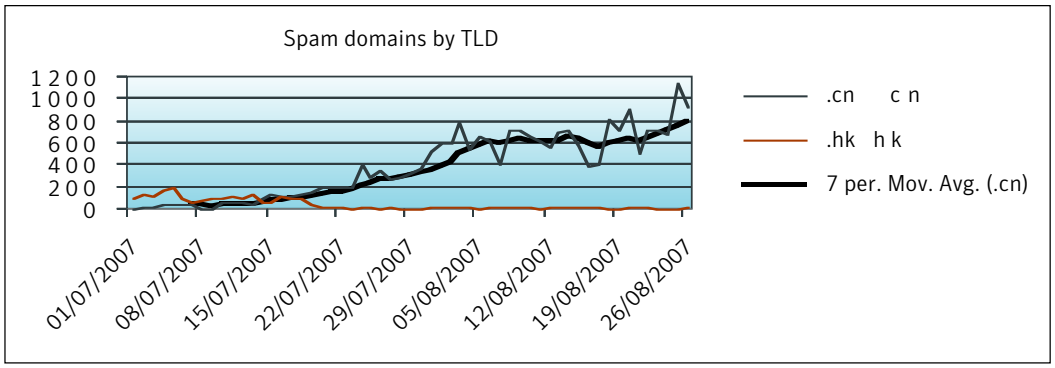
Infected machines become part of the botnet which is both responsible for sending these spam messages, and also hosting the Websites that cause malware to spread.

```
Subject: xxxx, who is that your with?
From: <xxxxx


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<body>
Dude I know thats you, someone emailed me a link to the video. see for yourself... <a
href="http://12.34.567.89/">http://www.youtube.com/watch?v=Qy2xM6esvMX</a>
</body>
</html>
```

Update: Spam Messages Containing URLS with Chinese Domains

In July, Symantec reported a significant increase in the number of spam messages containing URLs that use the top level domain (TLD) for China: 'cn.' August saw a seven-fold increase in spam messages that contain the 'cn' TLD.



These URLs are primarily being used to promote casino and pharmaceutical products. One of the more interesting pharmaceutical attacks purporting to be from the US NMA [National Medical Association] seemed to contain a URL with a 'com' TLD, but when clicked, referenced a 'cn' TLD URL.

```
We strongly
  recommend to visit our site before buying any medical products online</font>
<a href="http://yyyy.cn/?IJEMEOQkZWUlRfW1Z0XV5fVhpdWEVSVUwfXFZA"><font
color="#FFFFFF">.</font></a>
</p>
     <p><font color="#666666" size="2" face="Verdana, Arial, Helvetica, sans-serif">Our site <a
href="http:/yyyy.cn/?EILJSMQkZWUlRfW1Z0XV5fVhpdWEVSVUwfXFZA">http://www.yyyy.com/</a></font></p>
```

419 Scam Spam Hasn't Gone Away

One of the original types of spam messages—419 spam, named after an article of the Nigerian Criminal Code which deals with fraud—continues to innovate and evolve.

Twist #1: 419 Spammers Keeping Abreast Of Recent Spamming Techniques

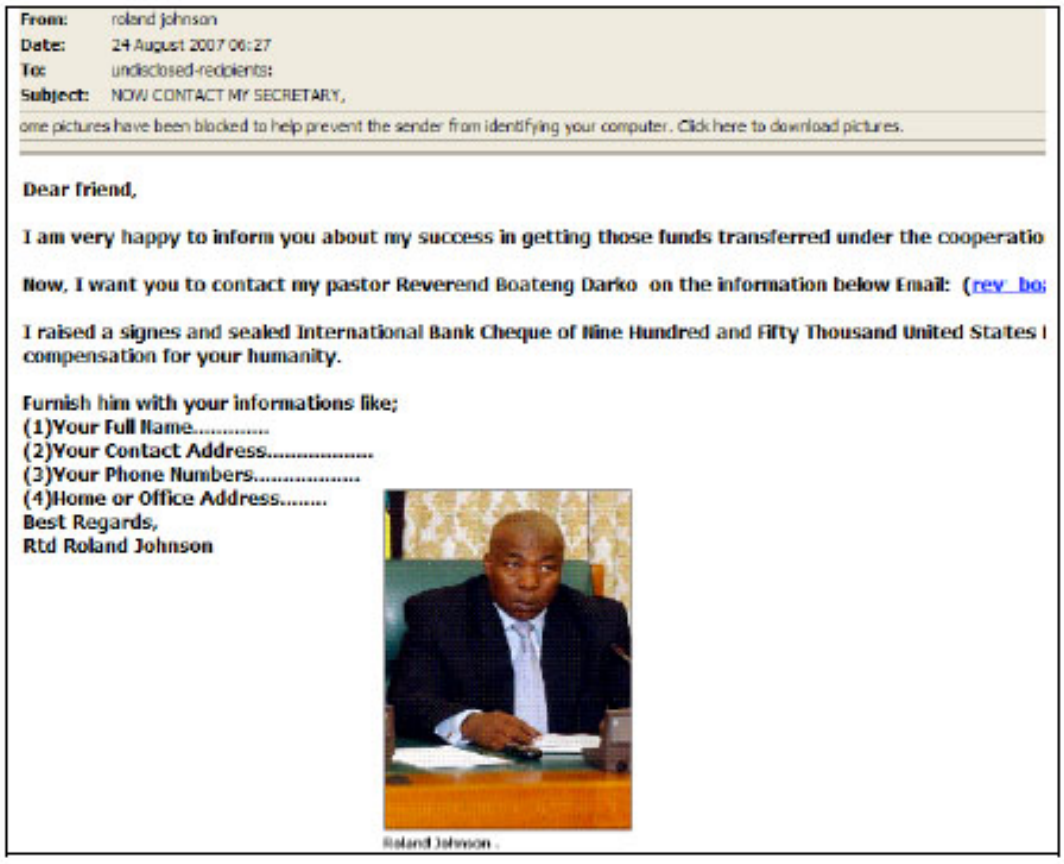
One interesting sideline to attachment spam is that 419 spammers have also started using Word file attachments. The spam messages use typical 419 subject lines:

> Subject: SOLICITING YOUR INTEREST AS THE NEXT OF KIN OF MY INHERITOR
>
> Subject: Dear Friend

The message bodies direct end users to open the attached Word file, which contains the 419 scam message.

Twist #2: Do You Know This Person?

Symantec has recently observed 419 spammers inserting images into their spam emails. In this specific attack, a JPG image of the person who claims to have transferred the money is attached.



From: roland johnson
Date: 24 August 2007 06:27
To: undisclosed-recipients:
Subject: NOW CONTACT MY SECRETARY,

ome pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

Dear friend,

I am very happy to inform you about my success in getting those funds transferred under the cooperatio

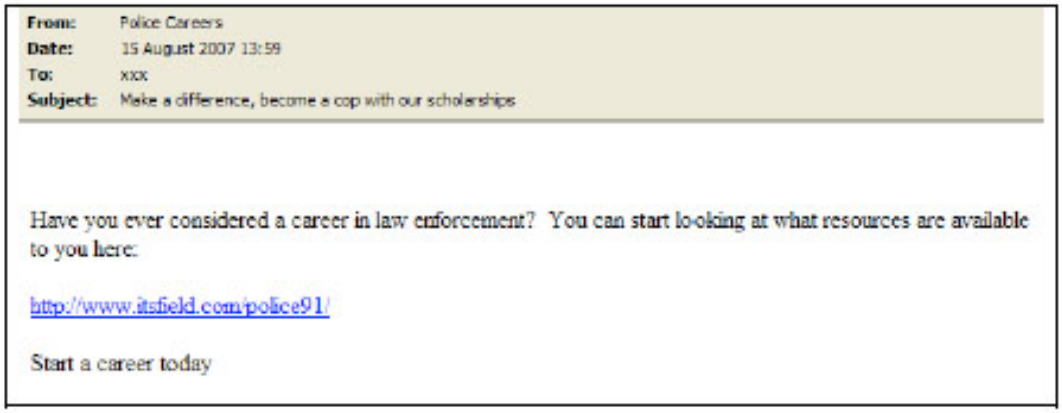
Now, I want you to contact my pastor Reverend Boateng Darko on the information below Email: (rev_bo;

I raised a signes and sealed International Bank Cheque of Nine Hundred and Fifty Thousand United States I compensation for your humanity.

Furnish him with your informations like;
(1)Your Full Name.....
(2)Your Contact Address.....
(3)Your Phone Numbers.....
(4)Home or Office Address.....
Best Regards,
Rtd Roland Johnson

Join The Police Force Spam

No, our law enforcement officers are not so hard up for recruits that they have taken to spamming. Instead, this is the latest career highlighted in degree spam. Symantec's filters blocked 130,000 of these messages in one particular attack.



From: Police Careers
Date: 15 August 2007 13:59
To: xxx
Subject: Make a difference, become a cop with our scholarships

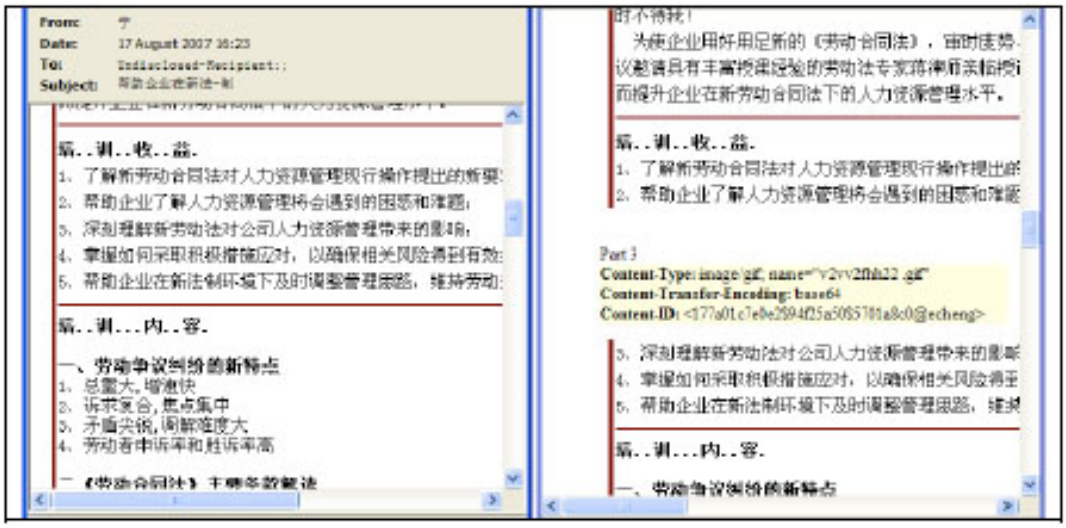
Have you ever considered a career in law enforcement? You can start looking at what resources are available to you here:

http://www.itsfield.com/police91/

Start a career today

Chinese Jigsaw Training Spam Images

Regional spam often follows trends observed first in English spam. One such example of this is a variation of a very typical Chinese spam for a training course, where the spammer has split an image into "jigsaw" pieces. Viewing the email in raw format, we can see the boundaries of each piece, but to the recipient it would appear as a single complete image. The objective of this is presumably to evade spam filters, but existing technologies are just as effective at detecting and blocking these messages.

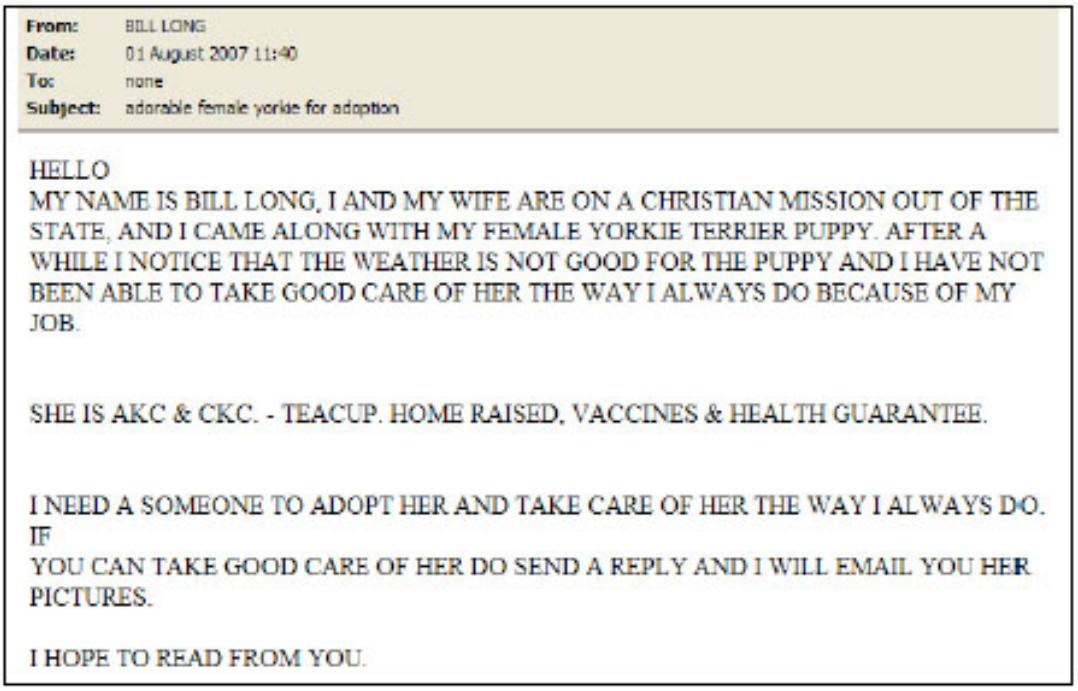


From: 宁
Date: 17 August 2007 16:23
To: Undisclosed-Recipient:;
Subject: 帮助企业在新法一制

Part 3
Content-Type: image/gif; name="v2vv20bb22.gif"
Content-Transfer-Encoding: base64
Content-ID: <177a01c7e8e2594f25a5055701a8c0@echeng>

Novel Puppy Scam Email

In this unsolicited message, the sender claims he wants to give away his pedigree puppy. It bears certain similarities to a 419 scam, with all shouting text and some incorrect English. It is likely that similar to a 419 scam, the next stage in the correspondence would be to ask any respondents for a financial contribution as a sign of trust.



From: BILL LONG
Date: 01 August 2007 11:40
To: none
Subject: adorable female yorkie for adoption

HELLO
MY NAME IS BILL LONG, I AND MY WIFE ARE ON A CHRISTIAN MISSION OUT OF THE STATE, AND I CAME ALONG WITH MY FEMALE YORKIE TERRIER PUPPY. AFTER A WHILE I NOTICE THAT THE WEATHER IS NOT GOOD FOR THE PUPPY AND I HAVE NOT BEEN ABLE TO TAKE GOOD CARE OF HER THE WAY I ALWAYS DO BECAUSE OF MY JOB.

SHE IS AKC & CKC. - TEACUP. HOME RAISED, VACCINES & HEALTH GUARANTEE.

I NEED A SOMEONE TO ADOPT HER AND TAKE CARE OF HER THE WAY I ALWAYS DO. IF
YOU CAN TAKE GOOD CARE OF HER DO SEND A REPLY AND I WILL EMAIL YOU HER PICTURES.

I HOPE TO READ FROM YOU.