The State of Spam

A Monthly Report – November 2007

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Charles Var
PR contact
charles_var@symantec.com

Contributors

Kelly Conley
Manager ESG
Symantec Security Response

Jitender Sarda
Manager Security Response
Symantec Security Response

Paresh Joshi
Email Security Analyst
Symantec Security Response

Francisco Pardo
Security Response Technician
Symantec Security Response

Niall O'Reilly
Security Response Technician
Symantec Security Response

Sammy Chu
Security Response Technician
Symantec Security Response

Robert Vivas
Sr Security Response Lead
Symantec Security Response

Kevin Yu
Security Response Lead
Symantec Security Response

Amanda Grady
Customer Response Analyst
Antispam Engineering

Takako Yoshida
Customer Response Analyst
Antispam Engineering

Shravan Shashikant
Pr. Business Intelligence Analyst
Antispam Engineering

Paras Gupta
Sr. Email Security Analyst
Symantec Security Response

Manish Satalkar
Email Security Analyst
Security Response

Monthly Spam Landscape

Ron Paul, MP3s, and global warming…what do they all have in common? No, it's not some new presidential campaign. They were all topics leveraged in new spam tactics in October. While overall spam levels continue to slowly inch upwards—70.5% of all email traffic in October—Symantec continues to observe spammers seeking out new alternatives to old favorites such as image spam and PDF spam.

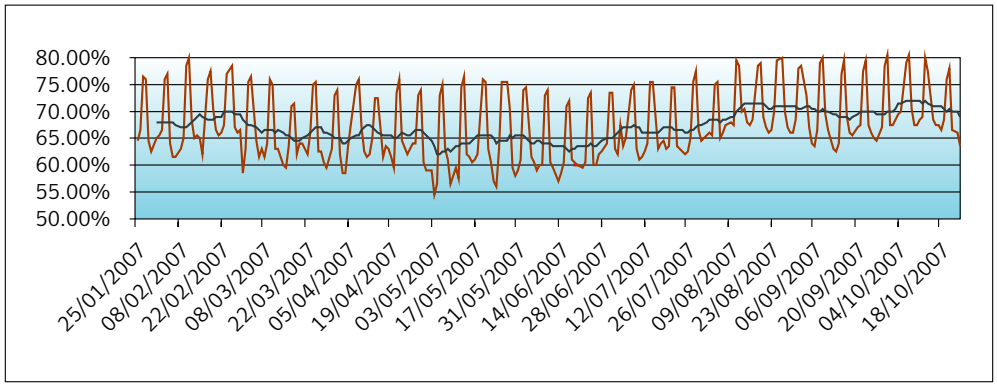
Highlights from this month included:

- **Spammers cast their presidential vote:** As the presidential campaigns heat up, one candidate receives an endorsement from a particular spammer. (See Page 6)
- **Fraud and scams on the rise:** These categories accounted for 18% of all spam in October. (up from 13% in September)
- **MP3 spam makes its debut**: Stock spam finally finds it's voice. (See page 7)
- **Click away the carbon" environmental spam:** With global warming making headlines nearly every day, spammers have taken notice and made this their latest social engineering tactic. (see page 8)
- **Image spam dips further:** Image spam which has tumbled dramatically since January 2007 continues to stagnate around 7% of total spam. (See Page 5)
- **Spammers exploiting Google searches:** Spammers have started using Google's advanced search operators to direct end users to a spam URL. (See Page 16)
- Additional insight is provided below on the following tactics:
    - Trick or Treat! Happy Halloween Spam
    - Spammers' Interest in the Housing Market Continues
    - Spanish-language Pharmaceutical Spam
    - Russian Bride Spam
    - Spam Spotlight: Regional Spam Trends APJ

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.



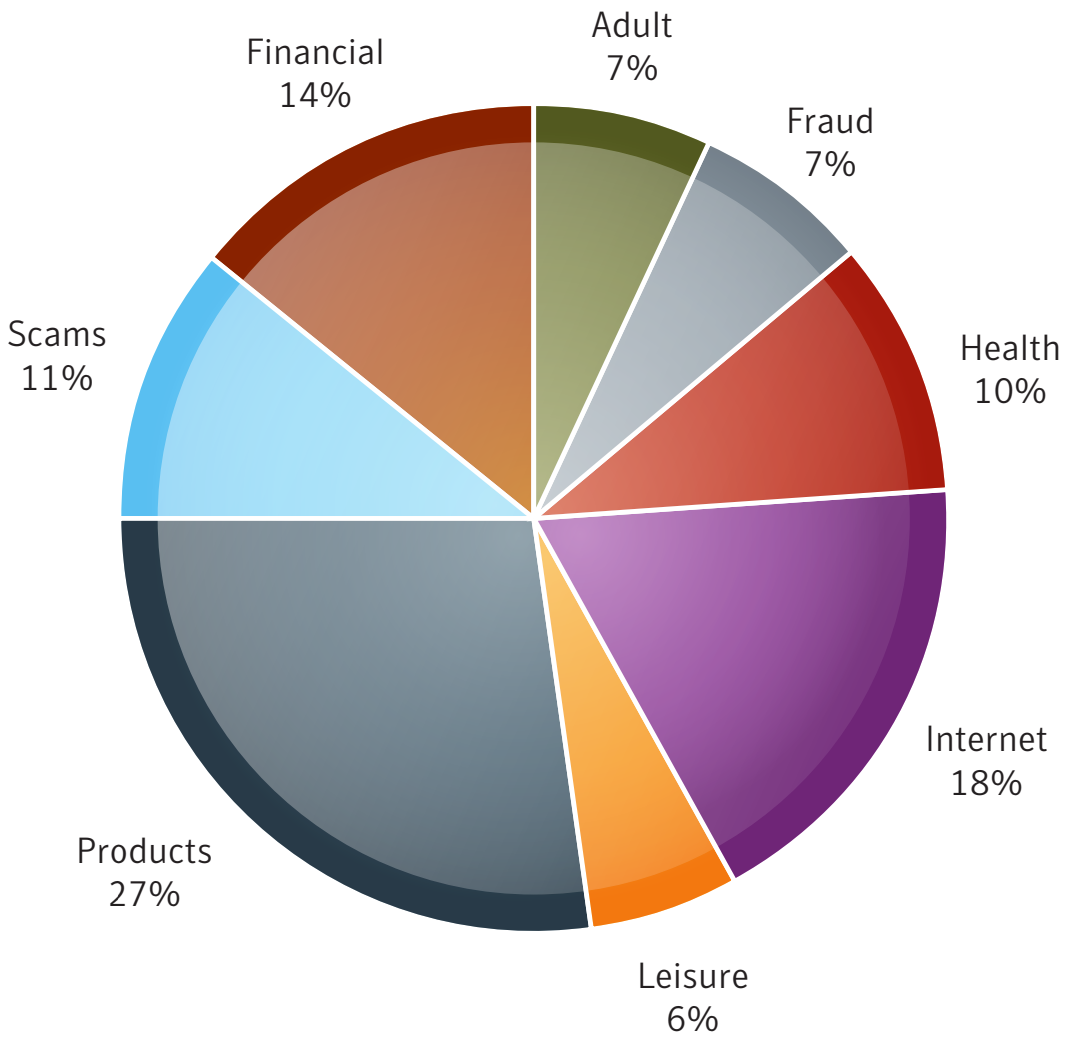
A trend line has been added to demonstrate a 7-day moving average.

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**

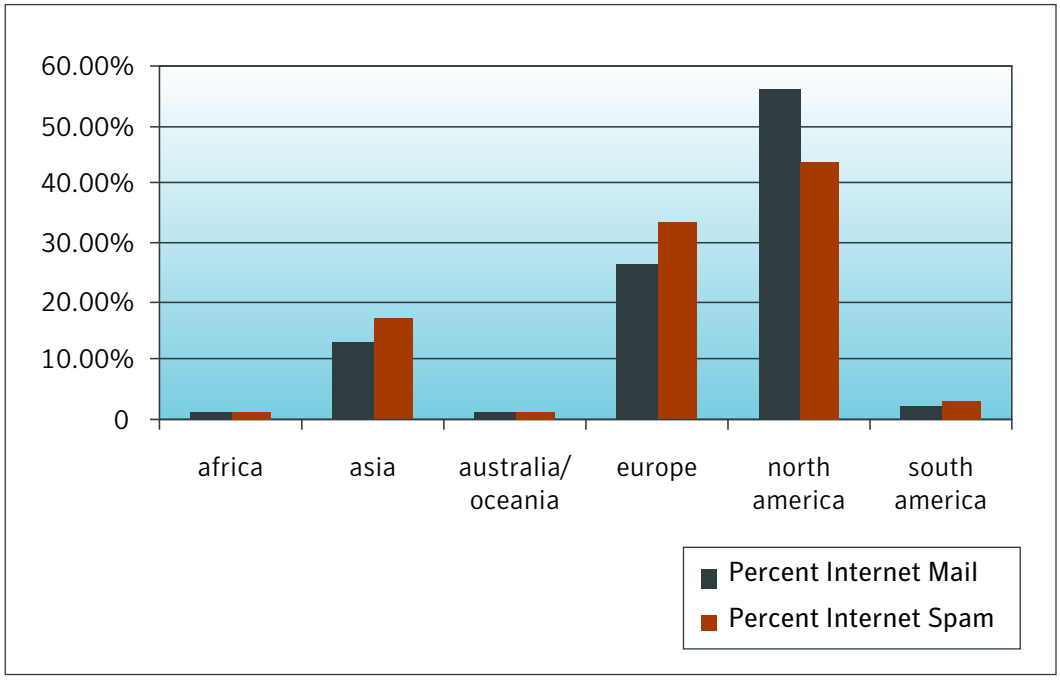
- **Spiritual Email attacks** with information pertaining to religious or spiritual evangelization and/or services. **Examples: psychics, astrology, organized religion, outreach**

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

Regions of Origin

Defined:

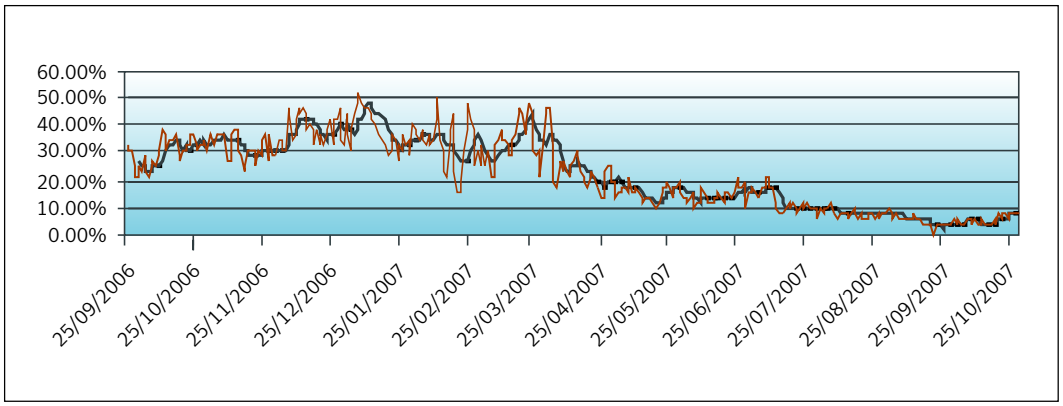
Region of origin represents the percentage of messages reported coming from each of the following regions: North America, South America, Europe, Australia/Oceania, Asia and Africa.



Percent Image Spam

Defined:

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



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

Spammers Cast Their Presidential Vote

As the presidential campaigns heat up candidate, Ron Paul, has become a particular favorite of one spammer. While there is no evidence to suggest that this particular spam campaign has emerged from Paul's campaign, it is an interesting signal of the type of spam emails that may emerge in the run up to the U.S. presidential election in 2008. Some of the subject lines in this spam campaign have included the following:

Subject: Government Wasteful Spending Eliminated By Ron Paul YyEQSCA
Subject: Iraq Scam Exposed, Ron Paul zdbSxxs
Subject: IRS Fears Ron Paul? SEzHlHR
Subject: Ron Paul Eliminates The IRS! YXAbFZT
Subject: Ron Paul Exposes Federal Reserve ybySNrt
Subject: Ron Paul Stops Iraq War! ZpmXrMW
Subject: Ron Paul Wins GOP Debate! yFlYaxM
Subject: Vote Ron Paul 2008! WtSktzm
Subject: Who Is Ron Paul? yyglMne

From:
Date: 29 October 2007 06:09
To:
Subject: Ron Paul Wins GOP Debate! BGxUwJY

Hello Scott,

Ron Paul is for the people, unless you want your children to have human implant RFID chips, a National ID card and create a North American Union and see an economic collapse far worse than the great depression. Vote for Ron Paul he speaks the truth and the media and government is afraid of him. This is the last honest politican left to bring this country out of this rut from the War Profiteers and bush Administration has created. Get motivated America, don't believe the lies of the media he has also WON the GOP Debate On Sunday! Value Freedom and Liberty instead of corporate lies and corruption. Bypass this media blackout they are doing to Ron Paul, tell your family and friends and get involved in a local group at meetup.com make your voice heard! He will end the War In Iraq immediately, He will eliminate the IRS and wasteful government spending, and eliminate the Federal Reserve and restore power to the people and the only person not a member on the CFR. Can any other runner make these claims or give Americans the true freedom we were all raised to believe? We are all economic slaves to the banks and the illegal federal Reserve. This is why our currency is worth nothing

MP3 Spam Makes Its Debut

Stock spam finally finds it's voice. Pump-and-dump stock spam has been one of the major types of spam observed by Symantec for some time now. Over the last year, Symantec has observed a change in the way that that these stock spammers try to bombard recipients with this type of spam. Examples include:

- In January, spammers predominately used images attached to spam emails to promote various stocks.
- In May, Symantec reported that spammers were using legitimate image upload hosting solutions to host images that referred to stocks.
- In June, Symantec reported an increase in spam which used links and embedded URLs to reference stock images contained in spam.
- In July, Symantec reported the emergence of attachment spam. PDFs and other file types were attached to spam emails. These PDFs contained information about various stocks.

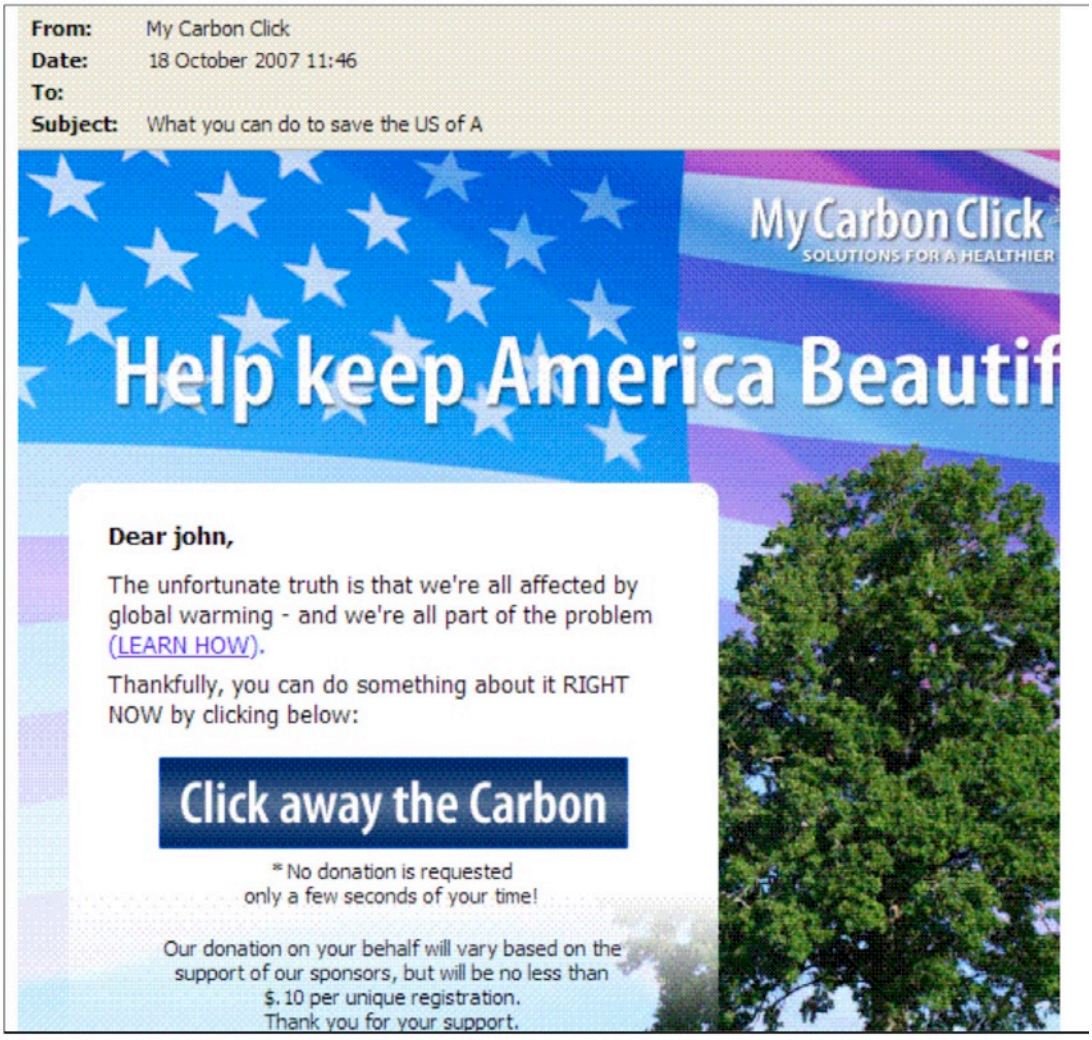
It comes as no surprise that in October, Symantec observed a small scale attack where MP3 files were used to promote specific stocks. The average size of the MP3 file was approximately 63.3 KB, with the garbled stock tip lasting for about 30 seconds. The audio content sounds as follows:

> "Hello, this is an Investor alert. XXXX Inc. has announced it is ready to launch its new XXXX.com Web site. Already a huge success in Canada, we are expecting amazing result in USA. Go read the news and hit on XXXX that Symbol get it XXXX Thank you"

As antispam filters become more sophisticated, it is clear that spammers will continue to reinvent how they send spam.

Spammers Care About the Planet Too!

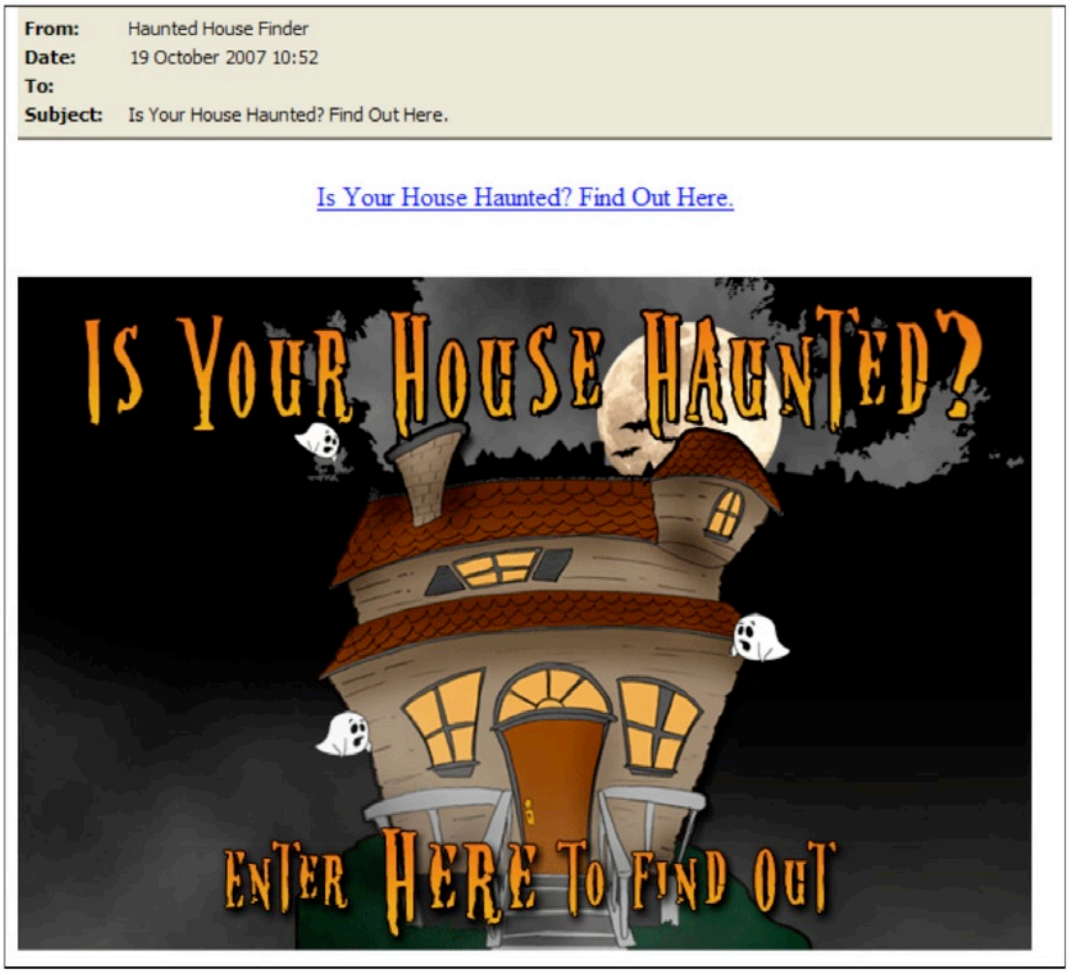
The issue of global warming has received an increased amount of press of late so it is not surprising that spammers too have begun to take an interest in this topic. A particular spam attack observed by Symantec in October offers a method that the recipient can use to "Click away the Carbon." On completion of a survey—which requests a significant amount of personal information—a donation "will be made" by one of the survey's sponsors on behalf of the email recipient. Again, spammers view this as a business, and therefore are motivated to leverage any hot topic that will generate the greatest response.



Additional Insights

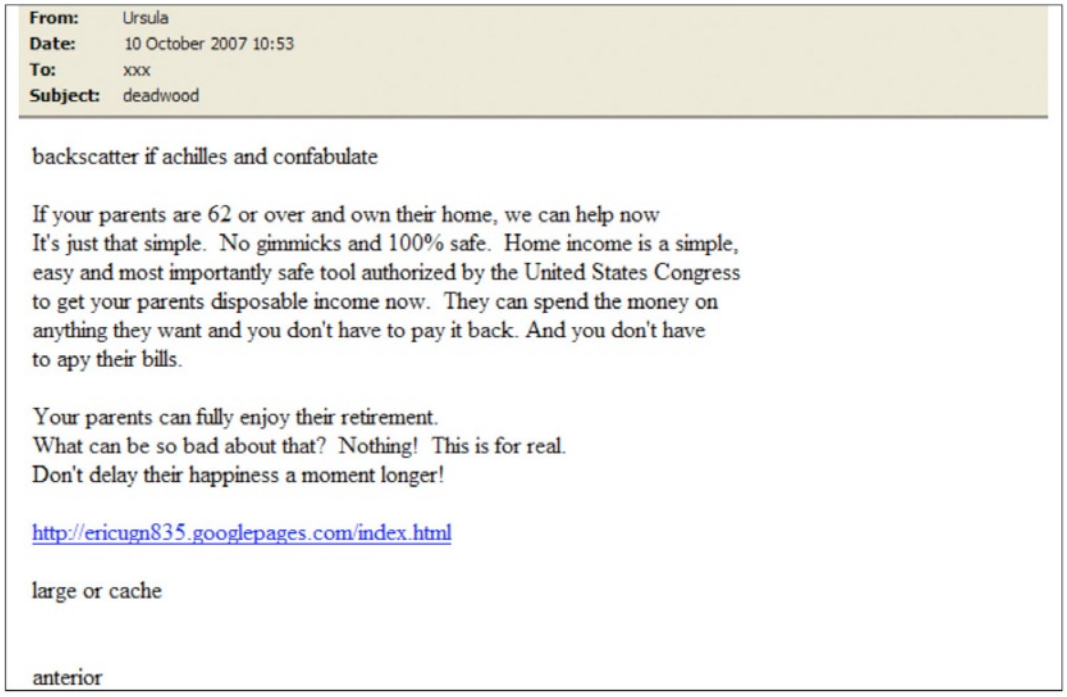
Trick or Treat! Happy Halloween Spam

Is your house haunted? One novel spam attack seen in the month of October purports to tell you for a mere $9.99/month (plus additional charges). With the subscription, you receive three text messages per month with tips about superstitions. Graphic heavy, this offer had the recipient answer several questions all revolving around popular superstitious beliefs such as 'have you broken a mirror?' and 'has a black cat crossed your path?' After answering the questions, one must input their mobile number and agree to the small print which states they are entering a binding agreement to pay $9.99/month for the three-times weekly text message service. Only after they agree to the subscription fees, would they receive the answers.



Spammers' Interest in the Housing Market Continues

Last month, Symantec reported how spammers had taken an interest in the housing market slowdown by offering different home refinancing deals. In an ongoing attempt to leverage capital by any means possible, the latest variations suggest releasing equity from your parents' home.



From: Ursula
Date: 10 October 2007 10:53
To: xxx
Subject: deadwood

backscatter if achilles and confabulate

If your parents are 62 or over and own their home, we can help now
It's just that simple. No gimmicks and 100% safe. Home income is a simple,
easy and most importantly safe tool authorized by the United States Congress
to get your parents disposable income now. They can spend the money on
anything they want and you don't have to pay it back. And you don't have
to apy their bills.

Your parents can fully enjoy their retirement.
What can be so bad about that? Nothing! This is for real.
Don't delay their happiness a moment longer!

http://ericugn835.googlepages.com/index.html

large or cache

anterior

Spanish-language Pharmaceutical Spam

Pharmaceutical spam has long been one of the most common types of spam in English. From time to time, Symantec sees attacks in other languages promoting medication products. In this Spanish example, a penis enlargement product with the sensationalist name of MagnaPene was found.

Although similar to English language attacks, there are some noticeable differences. In English versions of this attack, the email body generally would contain an advertising slogan, a URL, and some random words, whereas the Spanish version is written to appear more like a personal message. The translation of the sample below is:

Greetings,

Did you know that women love men that are well-equipped and skillful in bed ?

If you want to make happy hundreds of women in bed log on to
http://www.mprxdir.cjb.net

kisses sweetheart

From: Samanta Ortiz
Date: 08 October 2007 09:36
To: Recipients
Subject: estoy interesada en tu amistad

Te mando un saludo

Sabias que a las mujeres nos encantan hombres
bien dotados y habiles en la cama ?

Si quieres hacer felices a cientos de mujeres
en la cama entra a http://www.mprxdir.cjb.net

besitos corazon

Russian Bride Spam

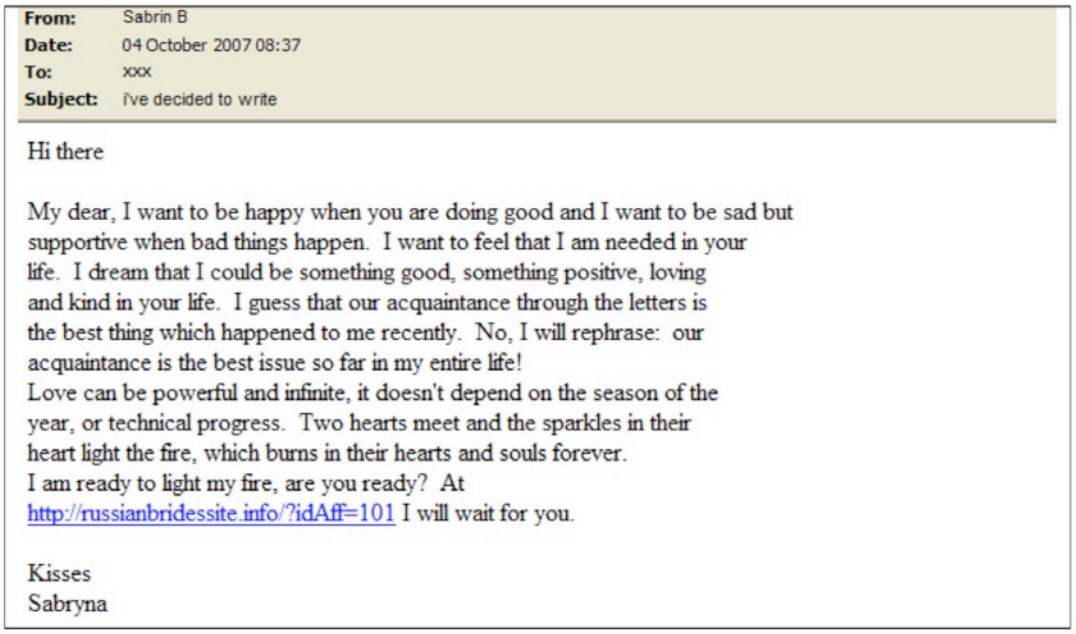
Throughout September and October, there has been a steady flow of dating spam attacks including "Russian bride" themed URLs, with a '.cn' or '.info' TLD. The headers are highly randomized, with URLs changing every 1-2 days. The attacks range from 100,000 up to 1 million messages, with the average attack at about 500,000 messages.

The attack has evolved from a short concise spam message...

From: Jillian Mcmanus
Date: 06 September 2007 20:09
To: xxx
Subject: Beautiful Russian women waiting to meet YOU!

Hello! dear Friend! Give we shall communicate?
http://russianbridespro.cn/?idAff=59
Best Regards Olga Elena

... to a longer, more subtle attack.



From: Sabrin B
Date: 04 October 2007 08:37
To: xxx
Subject: i've decided to write

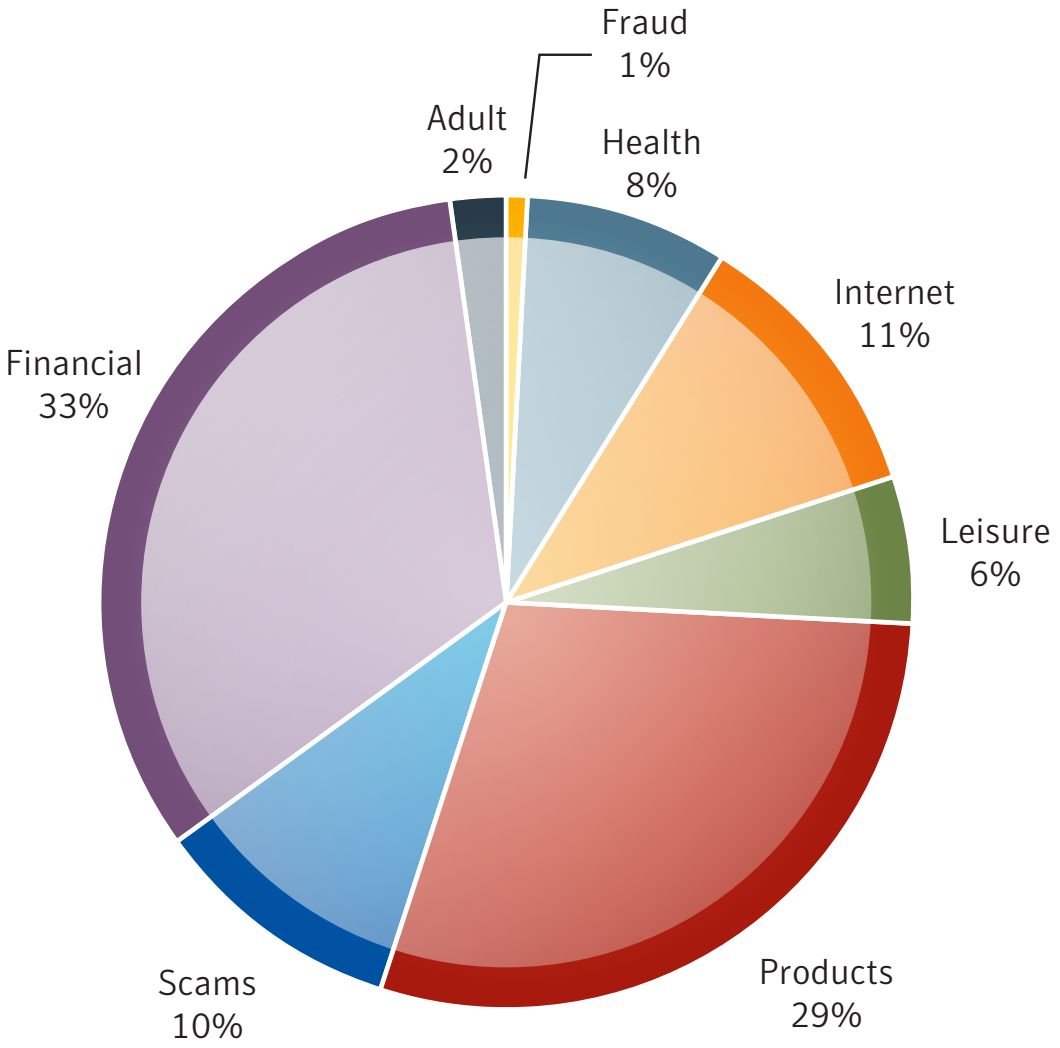
Hi there

My dear, I want to be happy when you are doing good and I want to be sad but supportive when bad things happen. I want to feel that I am needed in your life. I dream that I could be something good, something positive, loving and kind in your life. I guess that our acquaintance through the letters is the best thing which happened to me recently. No, I will rephrase: our acquaintance is the best issue so far in my entire life!
Love can be powerful and infinite, it doesn't depend on the season of the year, or technical progress. Two hearts meet and the sparkles in their heart light the fire, which burns in their hearts and souls forever.
I am ready to light my fire, are you ready? At http://russianbridessite.info/?idAff=101 I will wait for you.

Kisses
Sabryna

Spam Spotlight: Regional Spam Trends APJ.

A closer observation of spam tactics in APJ this past month revealed some interesting trends. Financial spam currently makes up 33% of all spam in APJ. This figure is contrasted by a global percentage of only 14% for financial spam. The adult and fraud categories in APJ also differ significantly from the global percentages. Adult spam makes up 2% in APJ compared with 7% globally and fraud makes up 1% in APJ compared with 7% globally. Some of the more high profile spam attacks in the APJ region are profiled below.



Chinese Invoice Spam

The classic invoice spam which is particularly prevalent in Chinese spam continues. The structure of this spam is quite similar to the structure of 419 spam.


尊敬的□□□□□□□□□□□□□□□

本公司……

□□□□□□□ 客□□□□□□□□□□□

□ 系 人 ：何生
□ □ ：136
E-mail ：xxxx

Translation:

Dear Person in charge (manager/finance) : Hello!

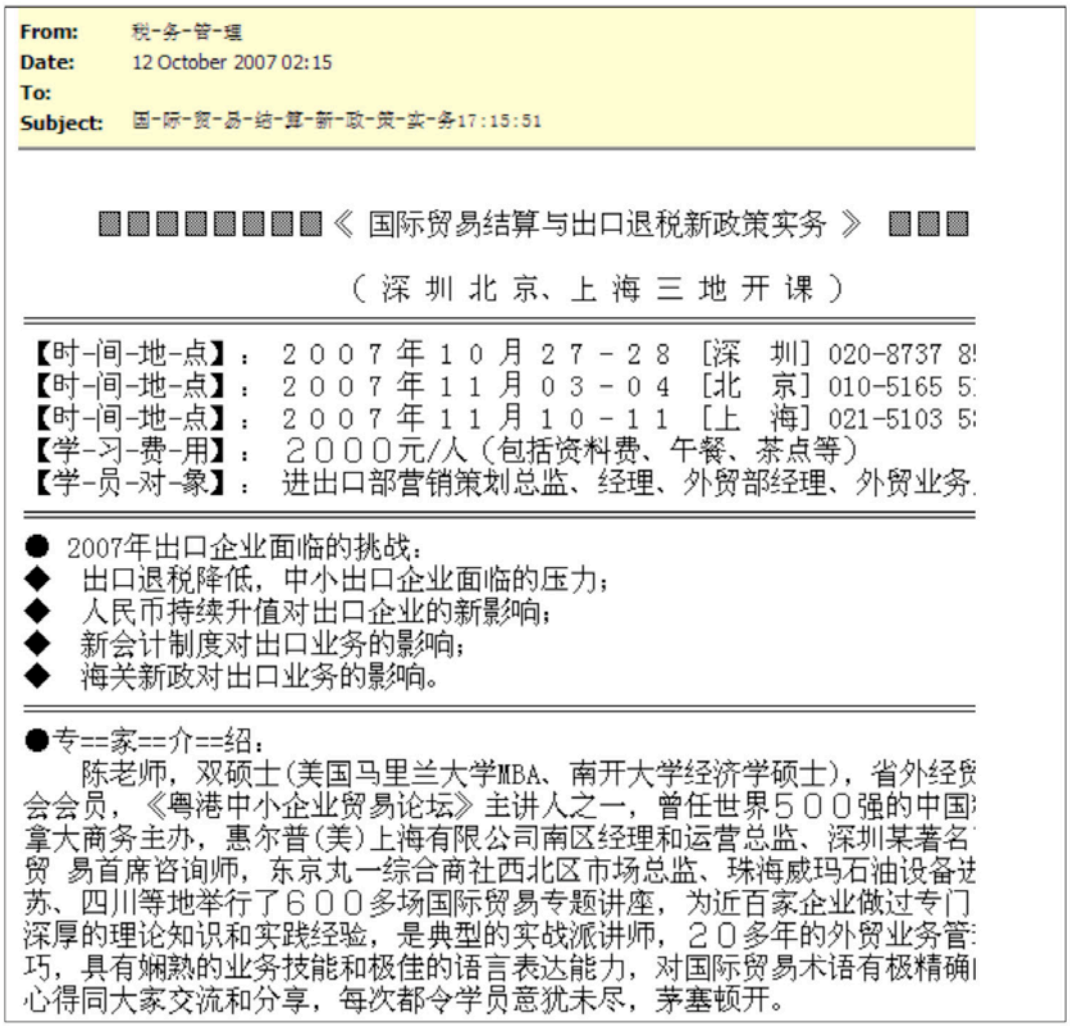
The body usually contain the term of the service

Please call!

Contact person: Mr. Ho
Phone number: 136
E-mail: xxxx

Seminar Promo Spam

Seminar promo ads spam is also very commonly seen in Chinese and Russian spam. Generally, this type of spam is not seen in English. It is often sent by certain management training institutions who are promoting training courses.



From: 税-务-管-理
Date: 12 October 2007 02:15
To:
Subject: 国-际-贸-易-结-算-新-政-策-实-务17:15:51

■■■■■■■■《 国际贸易结算与出口退税新政策实务 》■■■

（ 深 圳 北 京、上 海 三 地 开 课 ）

【时-间-地-点】： ２００７年１０月２７－２８ [深　圳] 020-8737 8
【时-间-地-点】： ２００７年１１月０３－０４ [北　京] 010-5165 5
【时-间-地-点】： ２００７年１１月１０－１１ [上　海] 021-5103 5
【学-习-费-用】： ２０００元/人（包括资料费、午餐、茶点等）
【学-员-对-象】： 进出口部营销策划总监、经理、外贸部经理、外贸业务

● 2007年出口企业面临的挑战：
◆ 出口退税降低，中小出口企业面临的压力；
◆ 人民币持续升值对出口企业的新影响；
◆ 新会计制度对出口业务的影响；
◆ 海关新政对出口业务的影响。

●专==家==介==绍：
陈老师，双硕士(美国马里兰大学MBA、南开大学经济学硕士)，省外经贸
会会员，《粤港中小企业贸易论坛》主讲人之一，曾任世界５００强的中国
拿大商务主办，惠尔普(美)上海有限公司南区经理和运营总监、深圳某著名
贸 易首席咨询师，东京丸一综合商社西北区市场总监、珠海威玛石油设备进
苏、四川等地举行了６００多场国际贸易专题讲座，为近百家企业做过专门
深厚的理论知识和实践经验，是典型的实战派讲师，２０多年的外贸业务管
巧，具有娴熟的业务技能和极佳的语言表达能力，对国际贸易术语有极精确
心得同大家交流和分享，每次都令学员意犹未尽，茅塞顿开。

Spammers Exploiting Google's Advanced Search Operators

Symantec has recently observed a trend where spammers are using Google's advanced search operators to direct end users to a particular spam URL.

The following is an example of a URL contained in a recent product spam attack

This URL is equivalent to typing

inurl:replica intext:"Perfect+cheap+replica+watches+online." into Google's search box

The Google query returns a link to a URL which is controlled by a spammer.

By using the Google search string spammers hope that some antispam URL technologies that require a precise URL path will have difficulty in filtering this spam attack. This is just another example of the steps spammers are willing to take in order to evade antispam filters.