SYMANTEC ENTERPRISE SECURITY

symantec™

Confidence in a connected world.

The State of Spam

A Monthly Report –

December 2008

Generated by Symantec Messaging and Web Security

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Monthly Spam Landscape

An important chapter in the history spam was written in early November 2008, when the percentage of email identified as spam dropped significantly due to the shutdown of McColo, which was allegedly hosting a significant number of botnet command-and-control systems. Recent spikes in spam volume indicate that a return to normal spam activity is in the works. While spam may have lost this battle, the spam war is certainly not over.

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

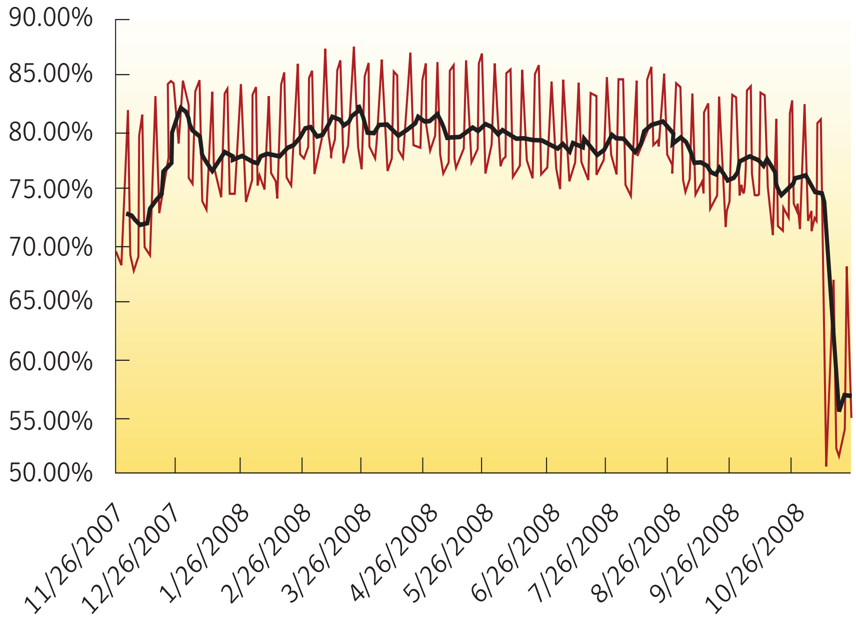
- **Hosting Company Shutdown Lowers Spam Volumes... For Now**
- **"It's beginning to look a lot like Christmas, ev'rywhere you go"**
- **Image Spammers Show There is Some Fight Left in the Old Dog**
- **Spammers Continue to Conduct Their Own U.S. Presidential Spam Campaigns**
- **Spammers Maintain "Acquaintance" With the IRS – in November!**
- **Can't Read English? Ecco lo Spam Italiano!**
- **Casino Spam Rolling Higher**
- **Mumbai Terrorist Attacks Bring Out the Worst in Spammers.**

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



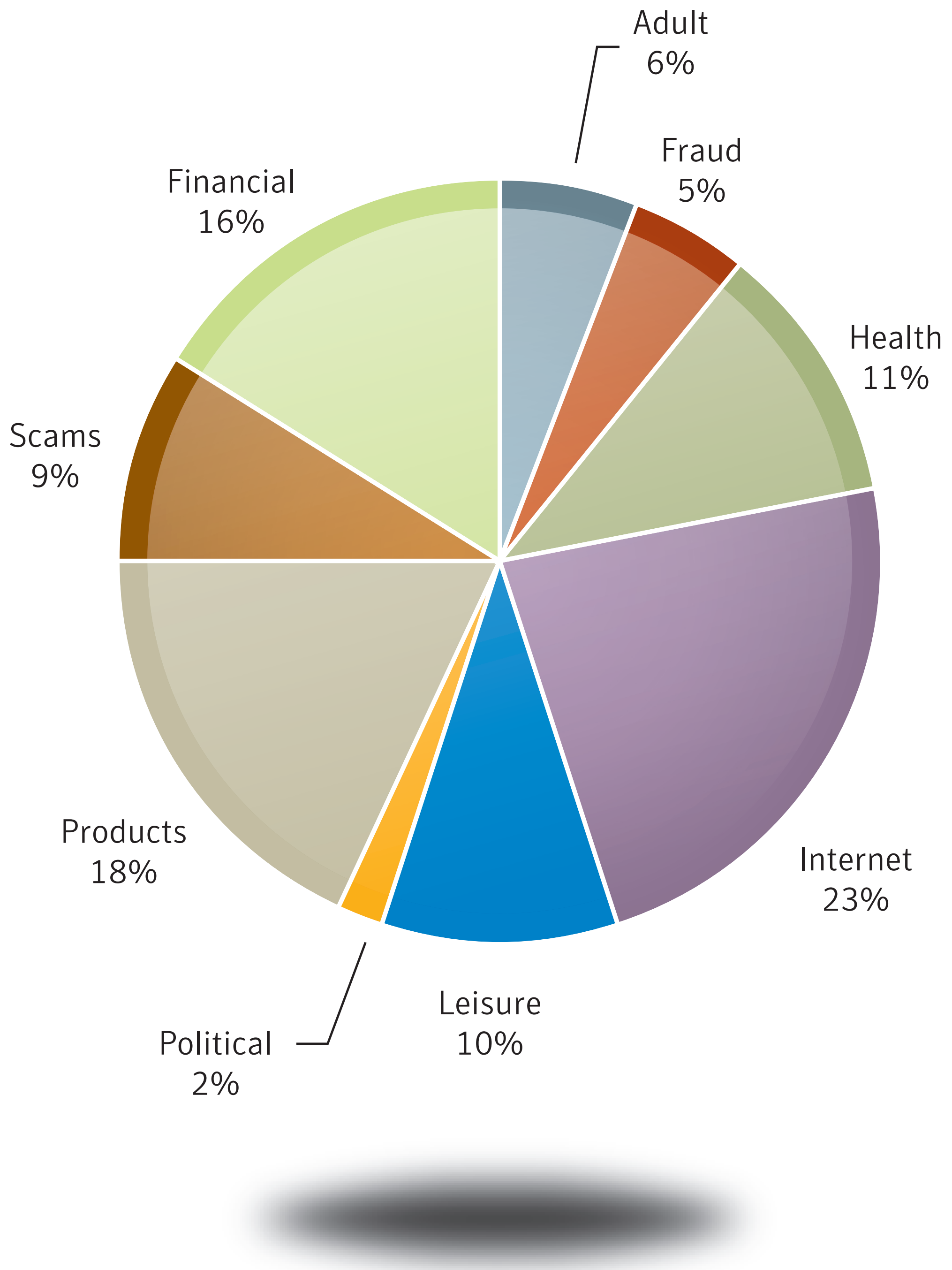
A trend line has been added to demonstrate a 7-day moving average.

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*

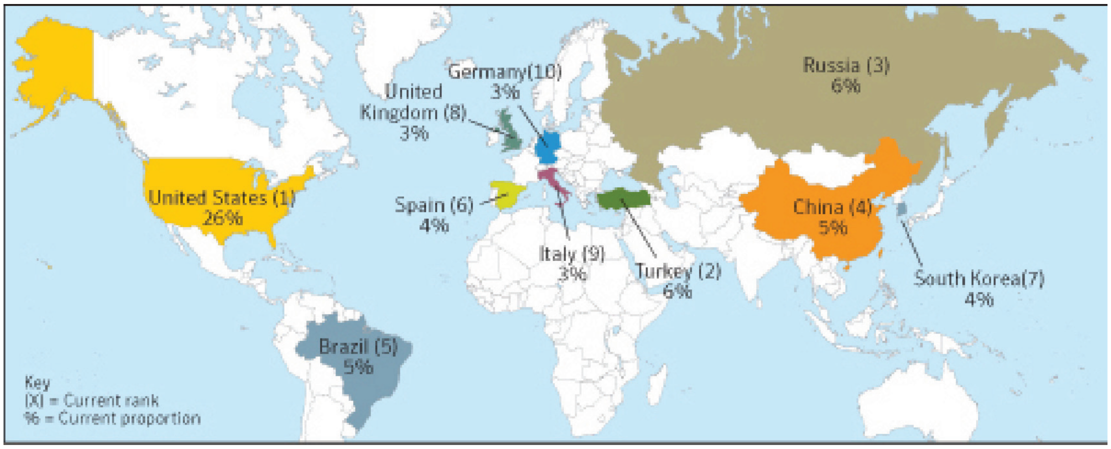
- **Spiritual E-mail attacks** with information pertaining to religious or spiritual evangelization and/or services. *Examples: psychics, astrology, organized religion, outreach*

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

Regions of Origin

Defined:

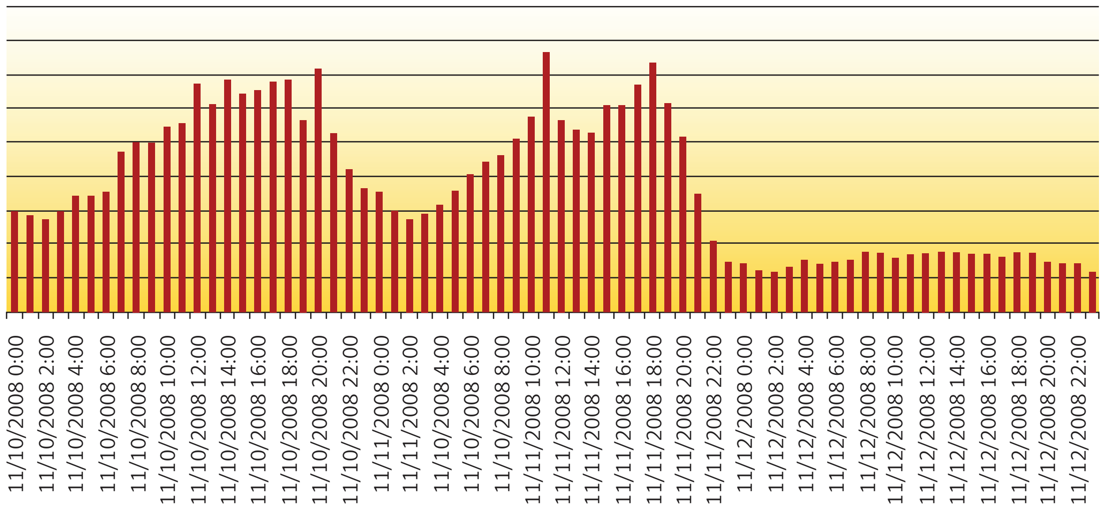
Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



Hosting Company Shutdown Lowers Spam Volumes... For Now

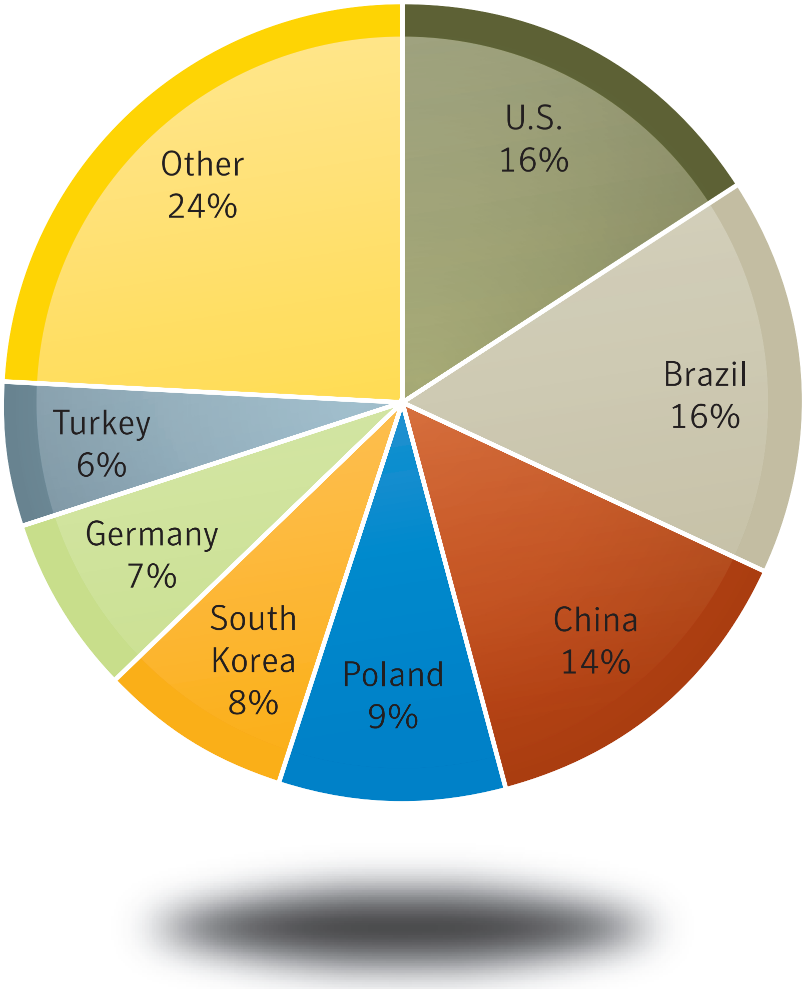
At approximately 21:30 GMT on November 11, 2008, multiple upstream network providers shut down access to McColo.com hosted systems, based on abuse complaints. One of the results of this action was a quick and dramatic decrease in spam sent worldwide. The volume change was measured directly in the Symantec probe network, which saw a 65 percent drop in traffic when comparing the 24 hours prior to the McColo.com shutdown to the 24 hours after.

The aftermath of the incident brought about several interesting findings. Among them was the fact that shutting down a single hosting company could have had such a large impact on overall spam volume. However McColo.com was allegedly hosting a significant number of botnet command-and-control systems, it is not surprising. Their IP range has, in the past, been linked with reports of serving up Rustock downloaders and also for controlling the spambot component. By cutting the link between these systems and the bot-infected machines they control, the ability to send spam from botnets such as Rustock and Srizbi can be significantly impacted. The speed with which spam volumes decreased also demonstrates the fact that while botnets are becoming increasingly robust, there are many that can still be impacted by losing a critical command-and-control link.



As November ended, Symantec observed that spam volumes had various upward spikes and were again creeping upwards. When Symantec examined the spam messages contained in the spikes, it was revealed that the spam messages were “Canadian Pharmacy” spam messages that were using short HTML messages with a varying set of domains in the URLs. During the spike, the percentage of spam messages containing the text/HTML content type mime part jumped to 55 percent of all spam. Prior to the McColo takedown, the overall percentage of spam messages containing the text/HTML content type mime part was over 55 percent, but after the takedown the average has been around 34 percent. The URLs in these spam messages contained hundreds of domains that used the Chinese top-level domain (.cn TLD). All of the name servers were hosted on either the same IP addresses as the domains, or additional IP addresses also located in China.

Source of Spam Volume Spike



In addition to the upward spikes in spam volumes, Symantec has also observed some recent spikes in percentage malware. This may point to more robust peer to peer bots in the future as spammers often need malware to push out those binaries.

These spikes indicate that a return to normal spam activity is in the works and it is certain that while this event may present an obstacle for spammers looking to get their message out in the short term, the profit motive still exists and will undoubtedly drive new spam campaigns.

"It's beginning to look a lot like Christmas, ev'rywhere you go"

It seems that no holiday season would be complete without spam messages offering a fake brand name watch or the like. Spammers have been busy for some time sending out their holiday-themed spam attacks. The top ten seasonal spam subject lines observed between October and November 2008 include the following:

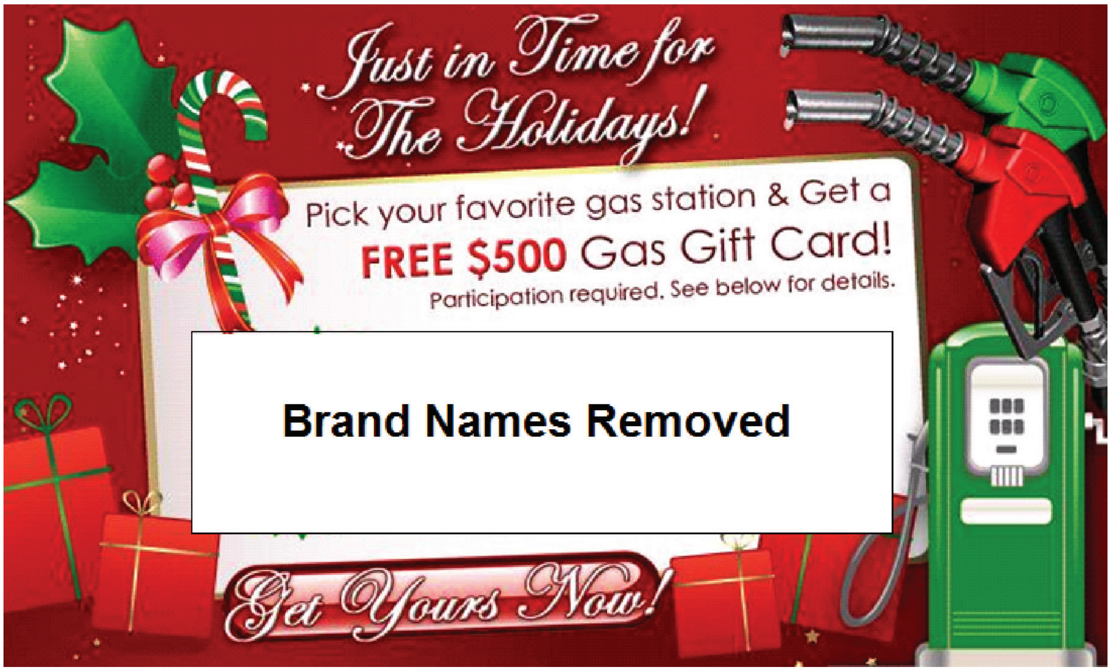
1	Best Sales 2008!
2	Spend less this Christmas
3	A Really Good Gift
4	Christmas Specials
5	Christmas promo few days left
6	Gifts for Christmas
7	Holiday Luxury Gifts
8	Hot Christmas Specials
9	Most Affordable Gifts
10	Low Christmas Pricing

Some interesting observations about these seasonal spam subject lines include:

1. As legitimate mailers send out more and more mailings with special "deals" and "offers" (as observed in the run up to Cyber Monday and Black Friday) to try and sell their products during this difficult economic time, spammers are using subject lines that try to draw users in by saving money. Seasonal subject lines are typically used in not only spam messages, but legitimate mailings.
2. These seasonal spam subject lines do not use randomization, and could typically be used by legitimate mailers. However, looking at some of these seasonal subject lines, certain patterns can be observed as spammers make slight changes to try and avoid certain anti-spam filters. Examples can be found below:

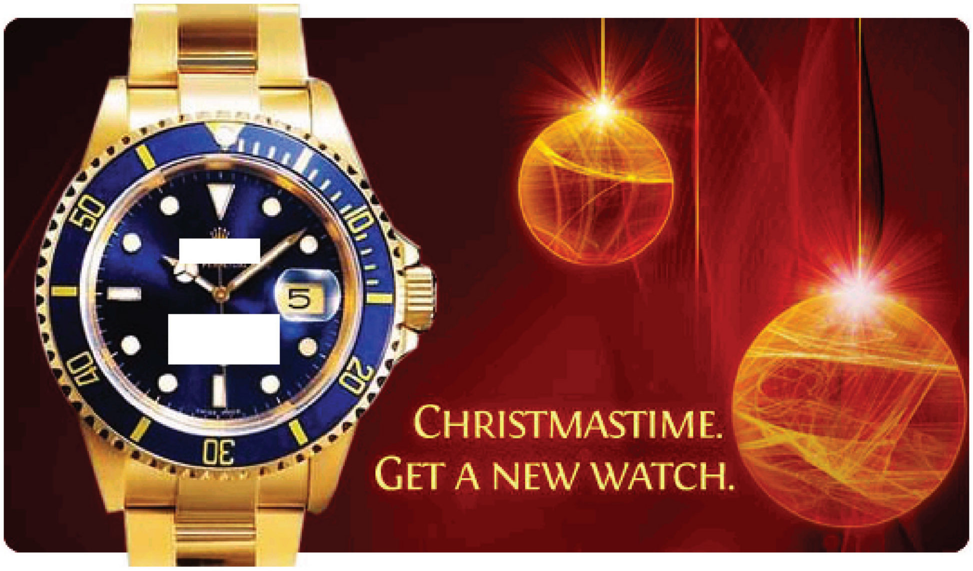
Subject: Amazing Christmas Deals
Subject: Amazing Christmas Specials

Holiday Spam Samples

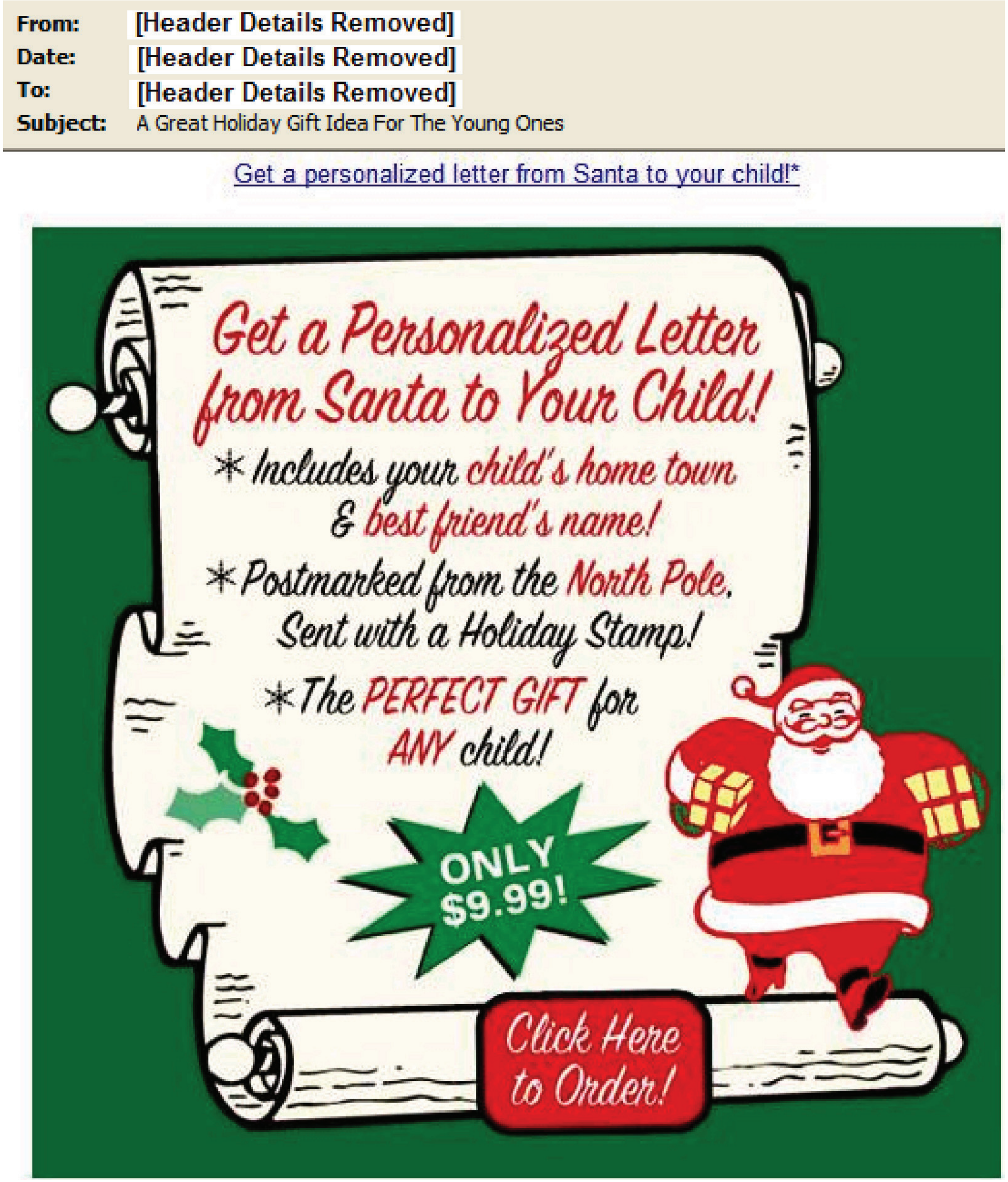

Just in Time for The Holidays!
Pick your favorite gas station & Get a
FREE $500 Gas Gift Card!
Participation required. See below for details.
Brand Names Removed
Get Yours Now!

Click here to get View Our Selection

We Carry Watches, Womens Bags and Much More
Tons of Great Gift Ideas!



Holiday Spam Samples

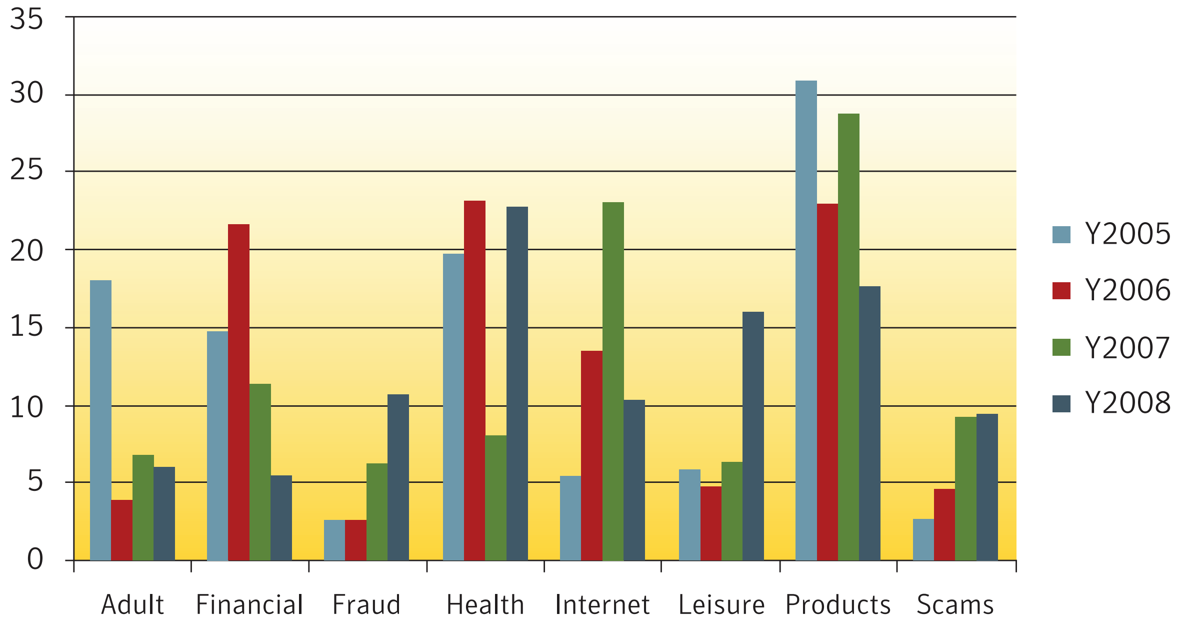


From: [Header Details Removed]
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: A Great Holiday Gift Idea For The Young Ones

Get a personalized letter from Santa to your child!*

Get a Personalized Letter from Santa to Your Child!
* Includes your child's home town & best friend's name!
* Postmarked from the North Pole, Sent with a Holiday Stamp!
* The PERFECT GIFT for ANY child!
ONLY $9.99!
Click Here to Order!

Spam Categories – Holiday Season

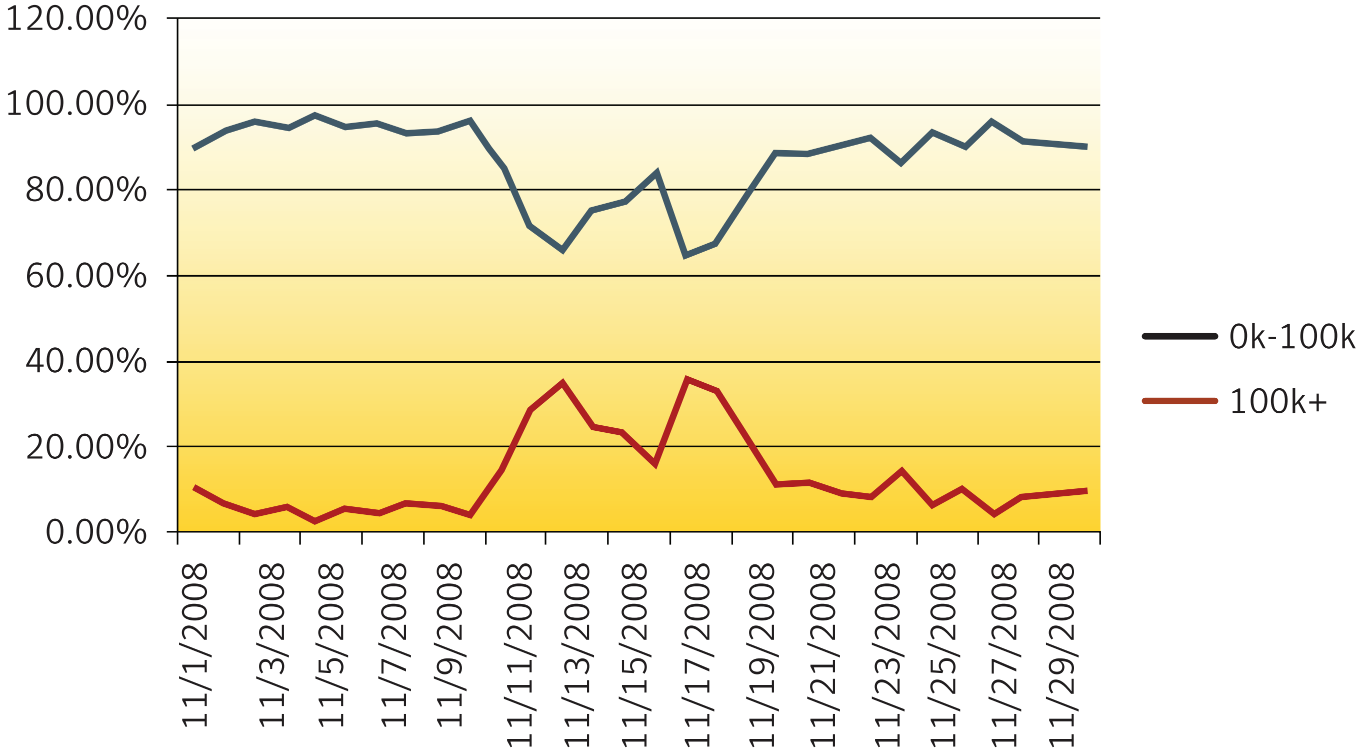


This chart shows that despite changing their spam tactics to try and evade antispam filters spammers continue to endeavor to deliver their spam messages. If only the Ghost of Christmas Past would haunt some of these spammers to try and prompt them to repent…

Image Spammers Show There is Some Fight Left in the Old Dog

Mark Twain once said, “It’s not the size of the dog in the fight, it’s the size of the fight in the dog.” This saying can be applied to image spammers. While image spam has not yet regained the dizzying heights of 2007 (when 52 percent of all spam was image spam), in November 2008, image spam hit a maximum of ten percent of all spam messages. Symantec observed a recent surge in spam messages using very large images. By analyzing image spam in November 2008, Symantec notes that over this period:

- 13.3 percent of image spam had a message size greater than 100kb
- 57.5 percent of image spam had an average size of between 10kb-50kb



When you consider spam messages in total for November 2008, the majority (79 percent) of messages fell into the 2kb-5kb range. As image spam continues to fight for its position within the “spamscape” it could indicate trouble for unprotected mail infrastructures.

Spammers Continue to Conduct Their Own U.S. Presidential Spam Campaigns

As President–elect Obama prepares for the beginning of his presidency, spammers continue to remind us that their presidential spam campaigns are not over. As John McCain ceded the election on November 4, 2008, spammers issued a new malicious code spam attack which included the subject line "Obama Wouldn't Be First Black President." The message noted that Barack Obama had been elected the 44th President of the United States. Recipients were encouraged to click on a link to, "Watch His amazing speech at November 5!" However, clicking on the video player downloaded malicious code. The body of the message can be found below:

> "Barack Obama Elected 44th President of United States
>
> Barack Obama, unknown to most Americans just four years ago, will become the 44th president and the first African-American president of the United States.
>
> Watch His amazing speech at November 5!
>
> Proceed to the election results news page >> [malicious URL removed]
>
> 2008 American Government Official Website - This site delivers information about current U.S. Foreign policy and about American life and culture."

In addition to the video, a Barack Obama Presidential Coin spam offer has emerged. The spam email which claimed to come from the New England Mint offers "a piece of history for only $9.95 plus shipping." The purpose of this spam message was to obtain credit card information from unsuspecting email users.

Spammers Maintain “Acquaintance” With the IRS – in November!

January to March is traditionally the time when taxpayers in the U.S. become reacquainted with their tax advisers as the mid-April “tax day” deadline looms. Unfortunately, this period has also become a time when phishing directed towards the IRS becomes more prevalent. As reported in the Symantec State of Spam report for April 2008, spammers continued to attempt to disguise themselves as the IRS, dangling an offer of a tax refund to unwitting recipients.

Imagine our surprise when we observed a phishing attack using the IRS brand in November—nearly five months before the next deadline for individual taxpayers. This phishing email indicated that the recipient was eligible to receive a tax refund and directed them to a website where the refund would be processed. The fraudulent site, branded with the IRS logo, is being used as a collection tool for credit card and other personal information.

The spam attack could be trying to take advantage of individuals who filed for a tax extension with an October 15th deadline and who might be looking for their tax refund. In addition, the IRS recently reported that it is looking for taxpayers who have not yet received their economic stimulus checks (checks totalling about USD $163 million were returned by the U.S. Postal Service due to mailing address errors). By law, economic stimulus checks must be sent out by December 31st of this year.

Email users beware of these attacks. If it looks too good to be true, then it probably is. As the IRS indicates on its website, it “does not initiate communication with taxpayers through email.”

Can’t Read English? Ecco lo Spam Italiano!

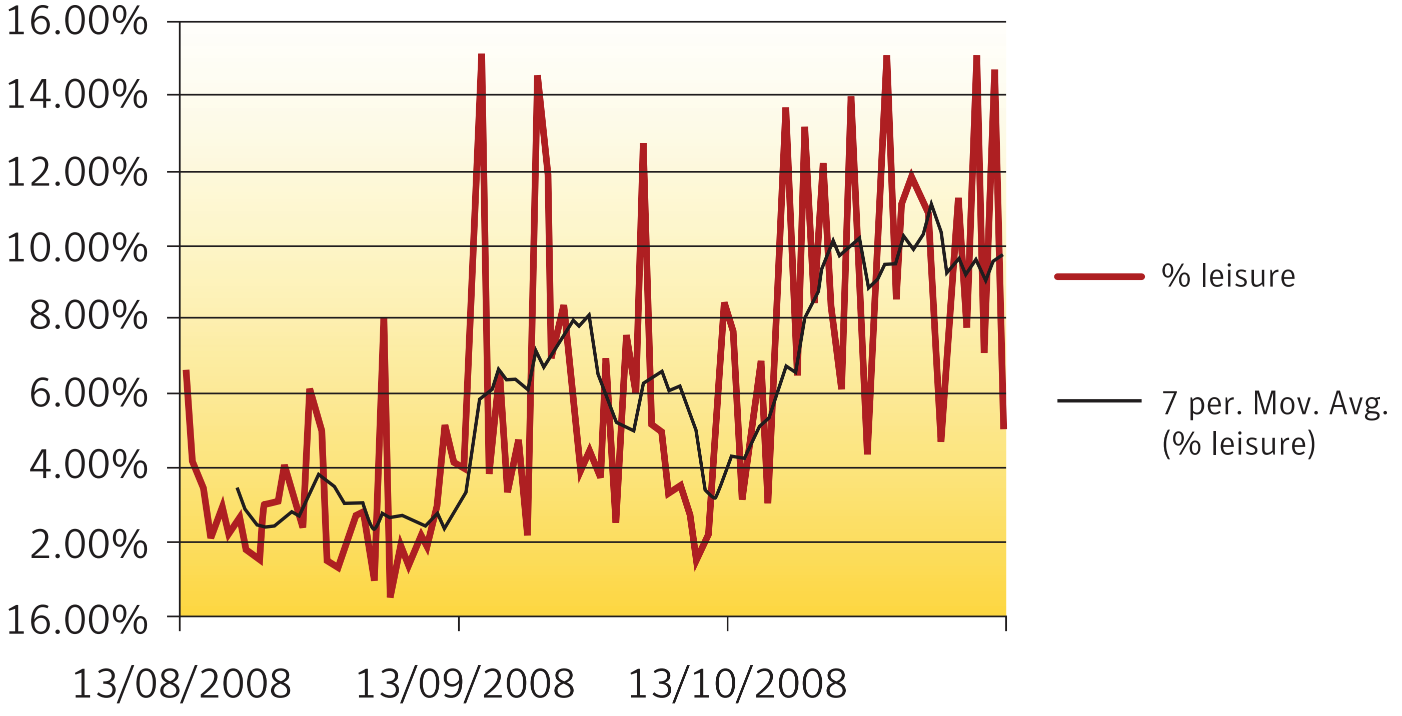
You may have come across multilingual translations of your favorite book or movie. It’s a sure fire way to extend one’s work to a wider audience. The desire for more money has driven spammers to employ similar tactics for their campaigns. Recent spam messages observed by Symantec included a work from home scam attack which offered a job that involved relaying payments between banks. In return, the recipient was allowed to retain a percentage of the amount transferred. This is a type of scam which involves the illegal activity of money laundering.

Initial English language spam attacks were soon followed by an Italian version within a space of ten days. The nature of the spam source (source IPs from different geographical locations) indicated that this attack was carried out through spamming bots.

> Italian Version Translation:
>
> “A prosperous business is looking for representatives. Our company was founded in 2004 and there are many of our representatives all over the world. If you have 3 hours free per week, you could start an international collaboration with our firm and earn more than $2,000. If you are interested in our vacancy, write to our email address developmentgrou@[message details removed] and we will send you more information.
> Please write your address et cetera…
> The [message details removed] Group”

Casino Spam Rolling Higher

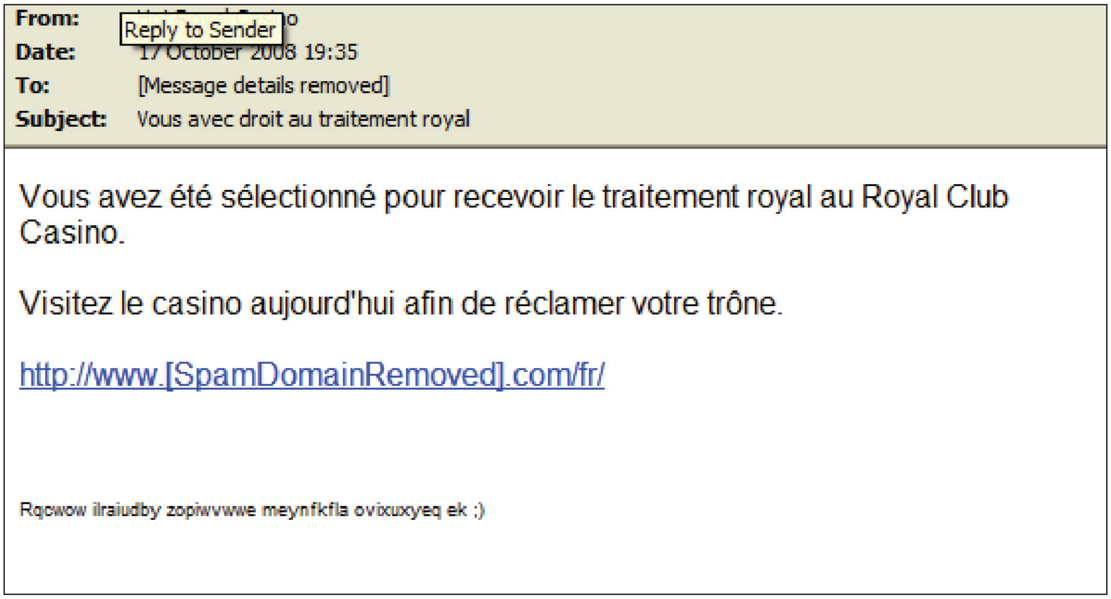
In recent weeks, Symantec has observed an increase in messages promoting online casinos, typically offering a cash bonus or VIP treatment. Leisure spam (defined as e-mail attacks offering or advertising prizes, awards, or discounted leisure activities) has accounted for up to 10 percent of spam globally during early November.



As we reported in the March 2007 State of Spam Report, these attacks are often translated into many different European languages in order to maximize the reach of the attack. The URLs are quickly changed from message to message, with a simple directory change for each European language – a French example is shown below. Spammers change the URLs frequently in order to try and stay ahead of URL-based antispam filters. Symantec uses more than 20 different filtering technologies in order to ensure comprehensive blocking of spam attacks, no matter what techniques spammers employ.

Despite the fact that online gambling in the US has many legal restrictions, most notably the Unlawful Internet Gambling Enforcement Act of 2006 which made transactions from banks or similar institutions to online gambling sites illegal, the restrictions haven't stopped spammers from targeting Americans, as clearly the potential size of the market is too large to ignore.

Free webhosting URL redirects have been notably used in spam attacks targeting the US market, presumably not just in an effort to evade spam filters, but also to make it more difficult to track down the hosts of the ultimate destination website.



From: Reply to Sender
Date: 17 October 2008 19:35
To: [Message details removed]
Subject: Vous avec droit au traitement royal

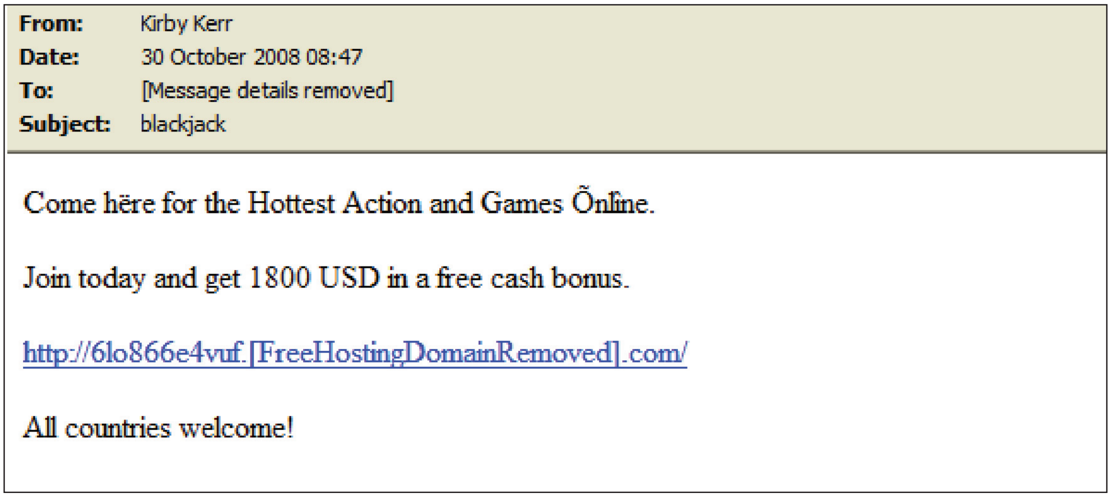
Vous avez été sélectionné pour recevoir le traitement royal au Royal Club Casino.

Visitez le casino aujourd'hui afin de réclamer votre trône.

http://www.[SpamDomainRemoved].com/fr/

Rqcwow ilraiudby zopiwvwwe meynfkfla ovixuxyeq ek ;)

In both examples shown, the objective of the email is to get the end user to download software running the various games. The software may attempt to steal sensitive information such as log-in credentials. However, don't be tempted by the offer of free money. In addition to the fact that a deposit is required in order to play, the terms and conditions state that 25 times the deposit and bonus must be wagered before cashing out – and it's likely the house will have long won by then.



From: Kirby Kerr
Date: 30 October 2008 08:47
To: [Message details removed]
Subject: blackjack

Come hëre for the Hottest Action and Games Õnline.

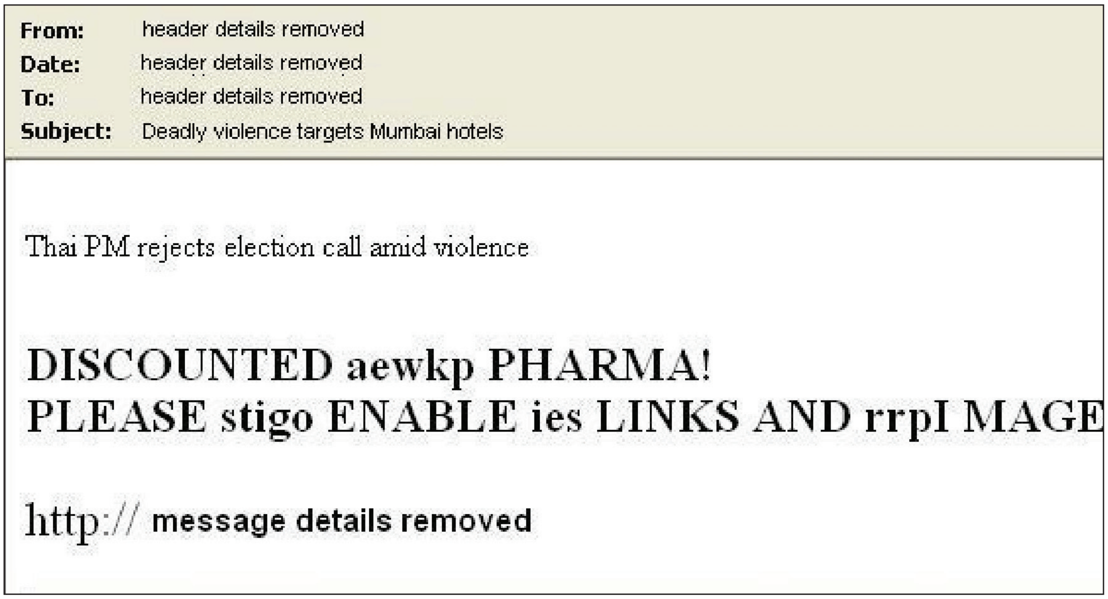
Join today and get 1800 USD in a free cash bonus.

http://6lo866e4vuf.[FreeHostingDomainRemoved].com/

All countries welcome!

Mumbai Terrorist Attacks Bring Out the Worst in Spammers.

India recently witnessed one of the worst terrorist attacks in Mumbai with hostage situations involving Indian and foreign nationals. Updates on the terrorists' activity were followed closely around the world. Unfortunately, this incident was also being followed closely by spammers who recently sent spam messages with subjects referring to the Mumbai attacks. The content of these messages were offering medication.



From: header details removed
Date: header details removed
To: header details removed
Subject: Deadly violence targets Mumbai hotels

Thai PM rejects election call amid violence

DISCOUNTED aewkp PHARMA!
PLEASE stigo ENABLE ies LINKS AND rrpI MAGE

http:// message details removed

This spam technique of using recent tragic news events has become a staple tactic for spammers. Among others events, spammers targeted the Burma cyclone and Chinese Earthquake earlier this year. Email users are advised not to click on links found in such spam emails.