SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

The State of Spam

A Monthly Report – February 2009

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

It's back – the war on spam's cat and mouse game continues. Spam volumes have continued to climb toward their pre-McColo shutdown levels, proving that as long as spammers continue to see a return on their investments, spam messages will continue to be sent in huge volumes.

The following headlines summarize the trends highlighted in the February 2009 report:

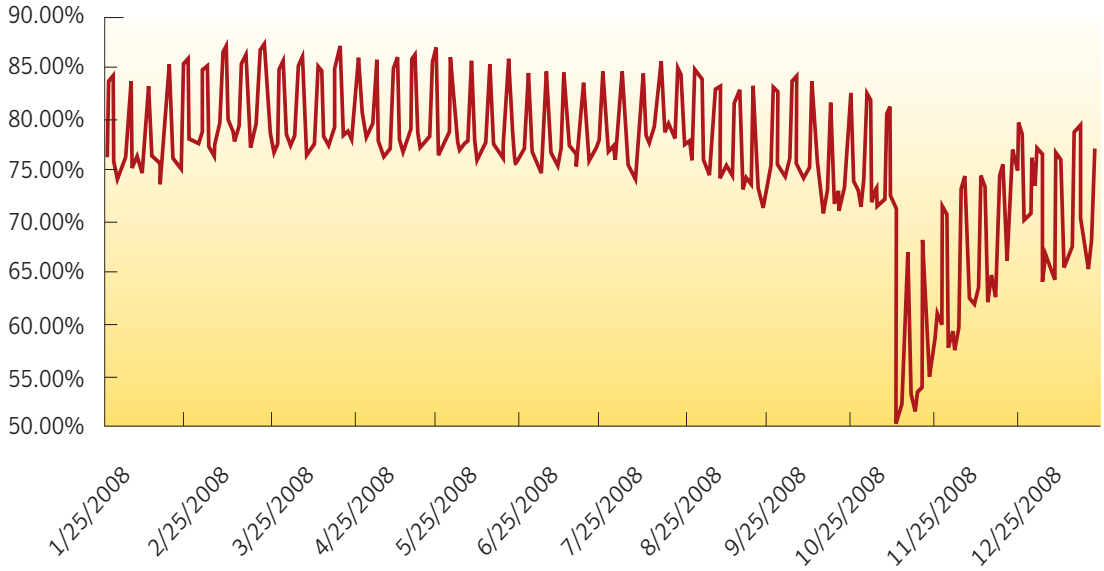
- **Spam's Insidious Rise to 'Normal'**
- **Need the Perfect Valentine's Day Gift? Spammers Provide Suggestions**
- **Year of the Ox Brings Continued Abuse of The cn ccTLD**
- **Spammer's Get Caught Up In Obamania During Inauguration**
- **Russian Spammers Are Waiting For Your Call**
- **The Underground Path to Illegal Gambling in China**
- **Keeping the Focus on Nigerian Spam**

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



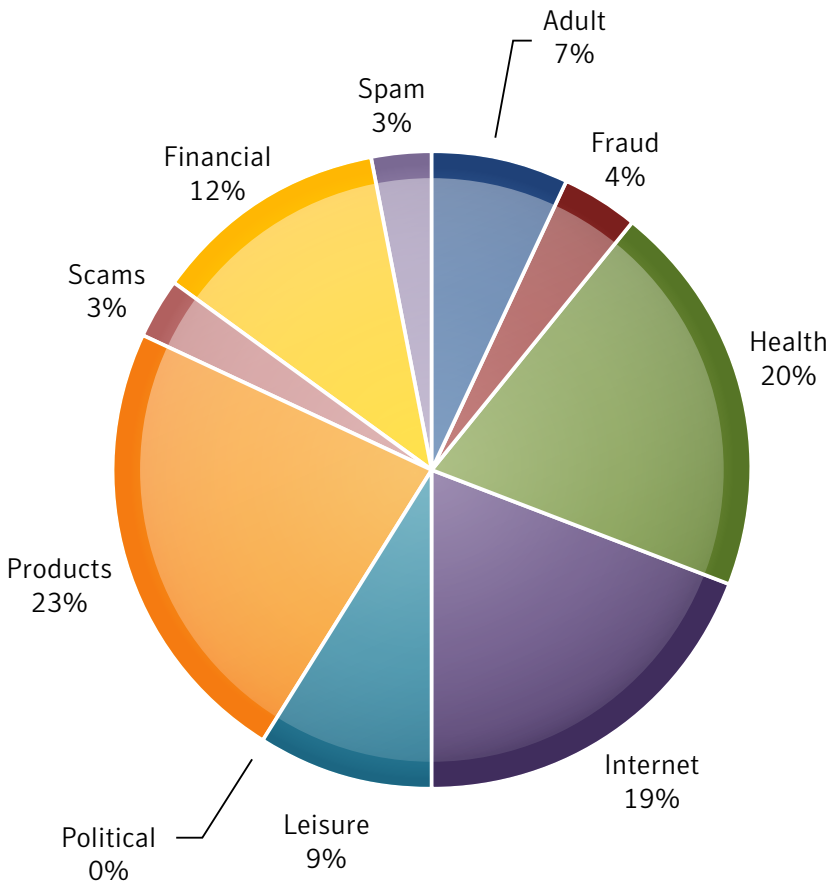
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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

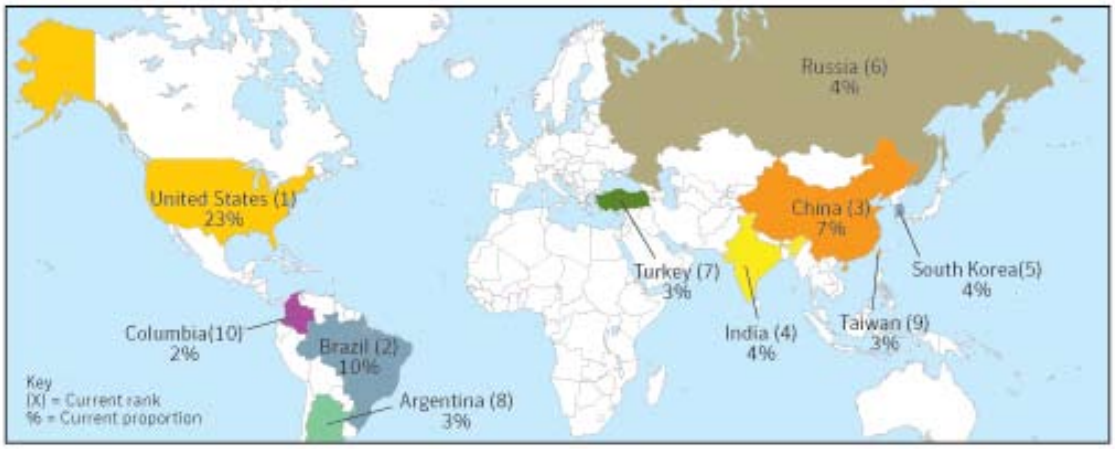
Global Spam Categories Last 30 Days



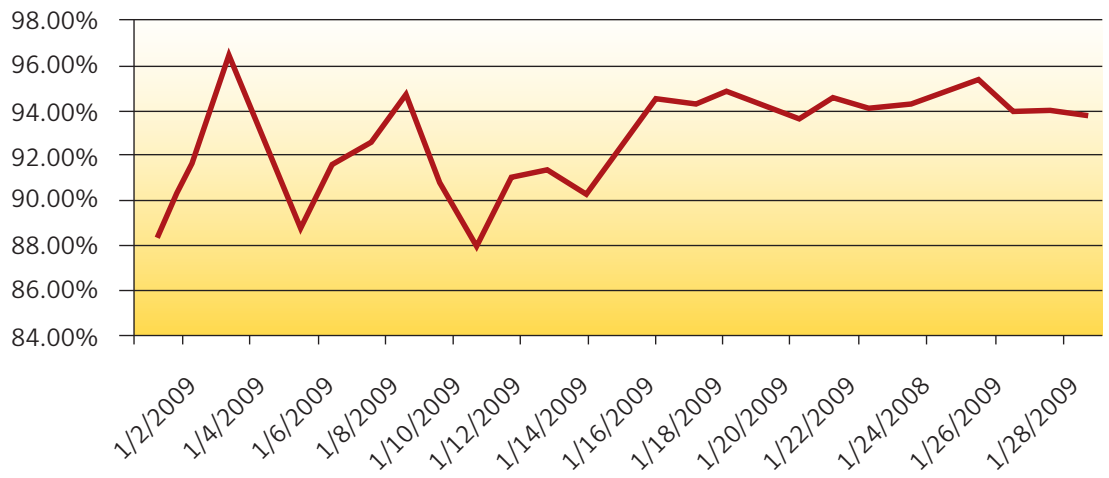
Regions of Origin:

Defined:

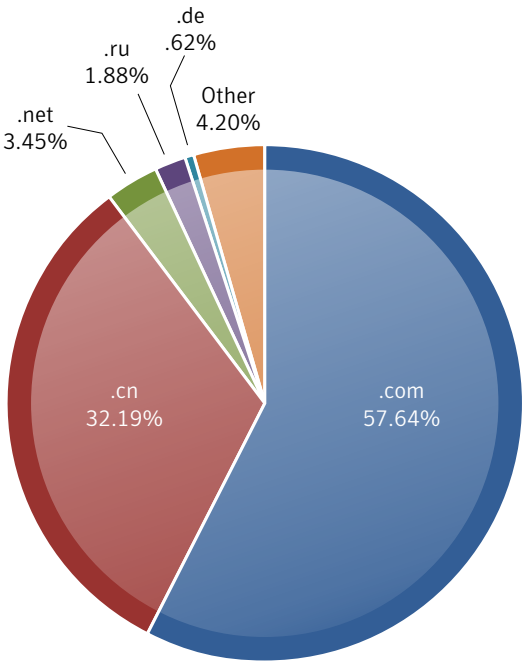
Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



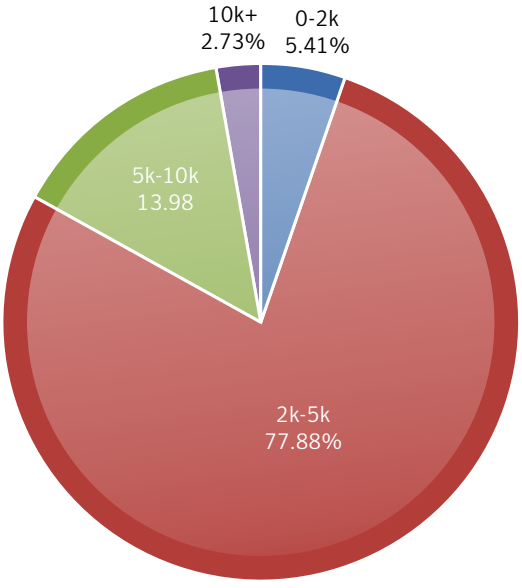
Percent URL Spam - January 2009



URL TLD Distribution
January 2009

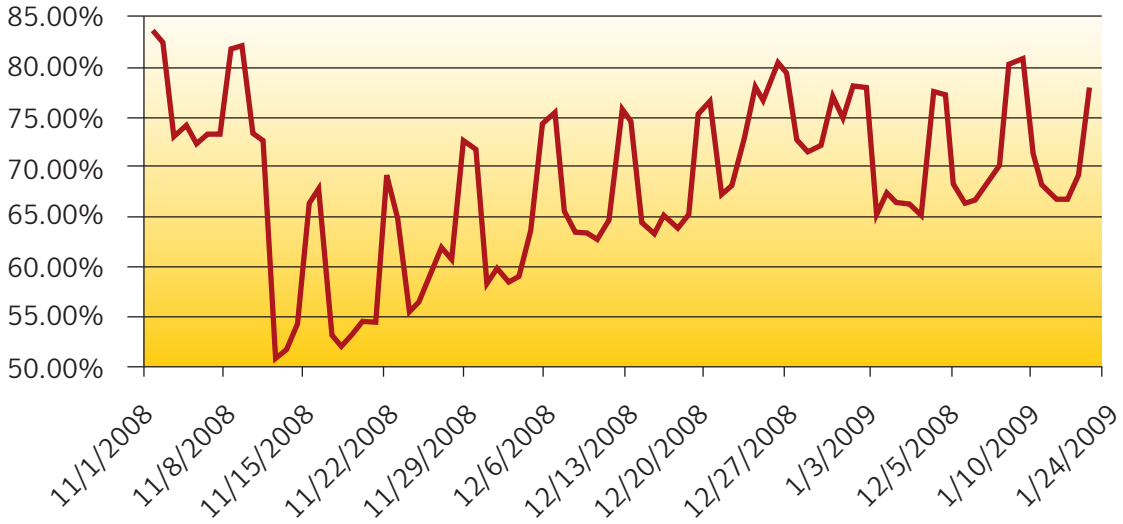


URL TLD Distribution
January 2009



Spam's Insidious Rise to 'Normal'

As predicted spam levels are continuing to rise post-McColo shutdown, accounting for over 79 percent of all email in recent days. When the McColo hosting company was shutdown on November 11, 2008, it was predicted that the event would present an obstacle for spammers looking to get their message out in the short term, but because the profit motive still exists for spammers, new spam campaigns have emerged. The speed with which spammers have returned to business is not totally unexpected. In October 2008, Symantec reported that the presence of active zombies around the world was shifting.

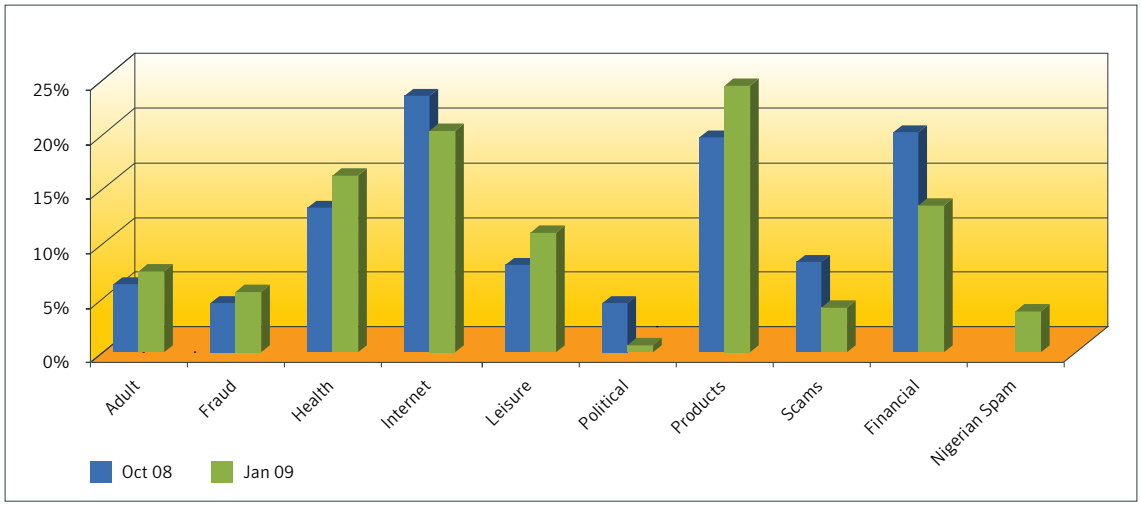


When the region of origin for spam was analyzed in January 2009, there were a few interesting findings. While the United States retains the dubious honor of primary region of origin for spam, and has consistently been one of the largest sources of spam, it has dropped three percentage points. Today 23 percent of spam messages originate from this region. It is expected that the overall share of spam originating from the United States will continue to decline over time as more people around the world come "online" in the 21st century.

New botnets in Latin America and Asia are increasingly driving spam campaigns post-McColo. Colombia and Argentina have joined the top ten region of origin for spam, while Brazil has climbed to second place behind the United States. Ten percent of spam originated from Brazil in the last month. For the past few months, India and China have both retained their positions among the top regions of origin for spam.

There are several reasons behind the shift in regional spam origin, but it is notable that investment in Internet and IT infrastructure for many countries spawns a massive growth in Internet users. Countries such as Brazil, India and China have a burgeoning middle class where Internet penetration is high and access to broadband is increasing. As IT security laws and regulations also vary widely around the world, an emphasis on security may not always be a primary concern.

In addition to the shift in the regions of origin for spam, a change in the type of spam message observed post-McColo has been observed. Between October 2008 and January 2009 we have monitoring the following changes in spam levels by category: Health (+3%), Leisure (+3%), Product (+4%), Financial (-5%), and Internet (-3%) spam.



Need the Perfect Valentine's Day Gift? Spammers Provide Suggestions

What would your Valentine like this year? Perhaps a shopping spree, a watch, cash, or an assortment of E.D. or weight loss pills?

With the onset of February, Valentine's Day spam is in full swing. Spammers have been busy making sure they have the perfect gift for your loved ones this year.

The top 20 Valentine's Day spam subject lines seem more like a laundry list of solutions for a cast of depressed porn stars than an array of truly romantic gifts. What says "Happy Valentine's Day" quite as well as "Hi Sweetie, here are some weight loss pills for you this year, maybe you can drop a few pounds!"?

The top 20 Valentine's Day-related subject lines for January

1-Increase your length, the best valentine's gift

2-Show off your length for valentine's

3-Get it before Valentine's day and watch her smile

4-You have been invited to partake in a shopping spree with [Removed] This Month for Valentines!

5-Happy Early Valentines Day, You have been selected to go on a $1000 Shopping spree to [Removed]

6-The Best Valentines Day Present Ever...

7-Your Valentines Day is about to get a lot better

8-Enjoy your Valentines Day with a Grand Cash from us =)

9-[Removed] invites you to take a $1000 shopping spree for Valentines Day

10-Great watches for your Valentine

11-Redeem Your Valentines Day Gift!

12-Buy a pair of watches for Valentine's Day

13-Free Shipping! Plus, Save on Valentine's Day Gifts

14-Make your Valentine happy with the perfect timepiece

15-Show the love. Give [Removed] this Valentine's Day.

16-Give a timepiece to your Valentine to keep track of time together

17-Valentines Day Approaching... Don't Miss Out on Our $1 Jewelry Auctions

18-Lose excess weight by valentine's day

19-An Erotic Valentines Gift

20-Need A Valentines Gift?

Holding the top three subject line spots is the male enhancement spam crowd who have really taken to this holiday and quickly adjusted their spiel to exploit it. Right behind them is the fake gift card gang and then the replica watch gang; after all, who could refuse a street-quality timepiece for Valentine's Day!

We have also seen an increase in subject lines in spam related to Valentine's Day that contain the following words and phrases:

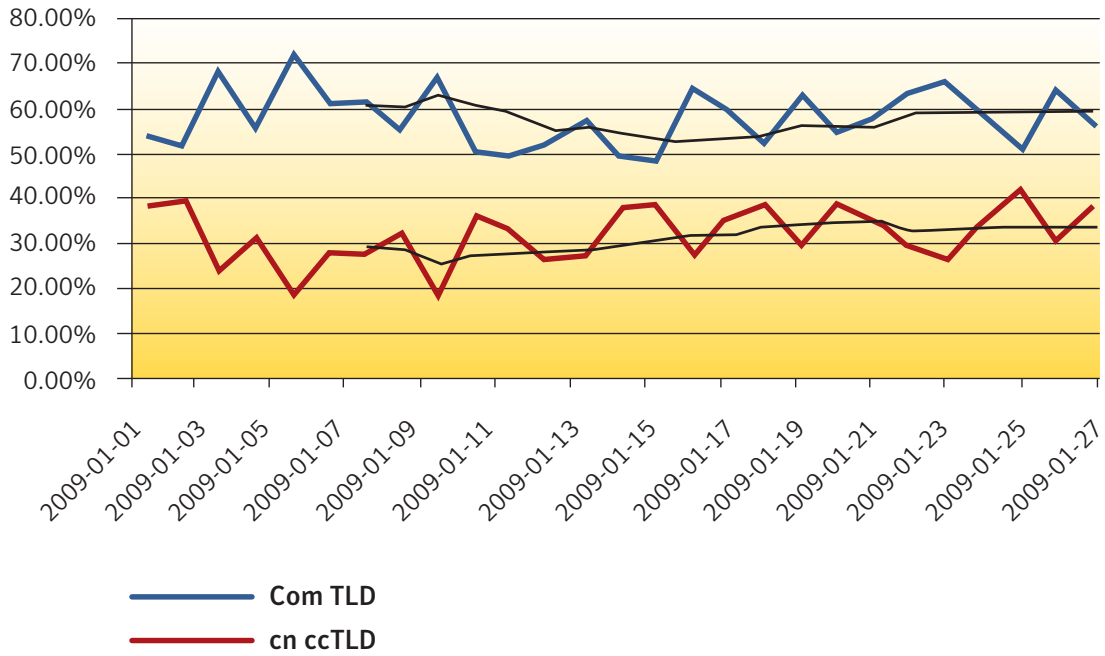
Feb 14
February 14
Cupid

With all of this preparation it is pretty obvious that there will be no shortage of fine romantic gifts this Valentine's Day!

Year of the Ox Brings Continued Abuse of The cn ccTLD

As the Chinese New Year /Spring Festival is celebrated around the world, a recent uptick in the abuse of the cn ccTLD which is reserved for China has been observed in spam messages. As noted in last month's report, approximately 90 percent of all spam messages contain some type of URL. In January 2009, an average of 32.5 percent of the URLs observed had a cn ccTLD, compared to an average of 57 percent of URLs, which had a com TLD. A top-level domain (TLD) is the part of a domain name that follows the final dot of any domain name. A country code TLD (ccTLD) is a top-level domain generally reserved or used by a country or a dependent territory.

URL TLD Distribution



Spammers often rotate domains and TLDs in their spam messages as they feel this tactic allows them to circumvent some antispam filters that depend on pattern matching to block the spam message. It has also been observed that spammers often switch TLD focus on an hourly basis. The URLs with a cn ccTLD observed recently have often tried to direct recipients to "offers" of pharmaceutical products.

Spammers Get Caught Up In Obamania During Inauguration

The U.S. Presidential election spam campaign which lasted from October 2007 until November 2008 was notable for the various angles used by spammers to try and evade antispam filters. The election spam campaign was dominated by the use of bogus news headlines and links to election-related videos that were cloaking malware. Spammers demonstrated their belief that the Presidential election campaign was a good vehicle to use to deliver their spam messages.

Recent Obama-related spam attacks have included messages offering "Our President - In His Own Words" or the ability to "Listen to President Obama's Audiobook." Spam messages offering "President Barack Obama Inaugural Dollar" and "Limited edition Obama coin now available to you" have been observed since November 4, 2008. In addition to these spam attacks, pharmaceutical spam has appeared which make suggestions such as "Even Obama uses this," "Obama's private video" and "Obama caught hot." The body of these particular spam messages contains advertisements for certain pharmaceutical products.

As the world counted down to the inauguration of the 44th President of the United States, it seemed that certain online miscreants became swept away by Obamania as a new wave of malicious spam messages with a "Presidential theme" were distributed.

Subject: You must look at this! Our new president has gone Yours truly,
Subject: Breaking news Barack Obama refused to be the president of the United States of America Yours Sincerely,
Subject: Breaking news There is no president in the USA anymore With kind regards,
Subject: What is going on with our country? Obama has gone

Each of these spam emails contained a hyperlink that, when clicked on, directed the user to a Web page that looked very similar to the official Obama-Biden campaign site. The site first attempted to exploit weaknesses in Web browsers to surreptitiously install malware onto machines. Even if the machine was fully patched, the spammer hoped that human curiosity would prevail, and therefore every hyperlink on the site pointed to malware.

The files available for download from the site included names such as usa.exe, obamanew.exe, pdf.exe, statement.exe, barackblog.exe and barackspeech.exe. This piece of malware was identified under the name W32.Waledac and was capable, among other things, of harvesting sensitive information, turning machines into a spam zombie and establishing a back door into computers that would allow it to be remotely accessed.

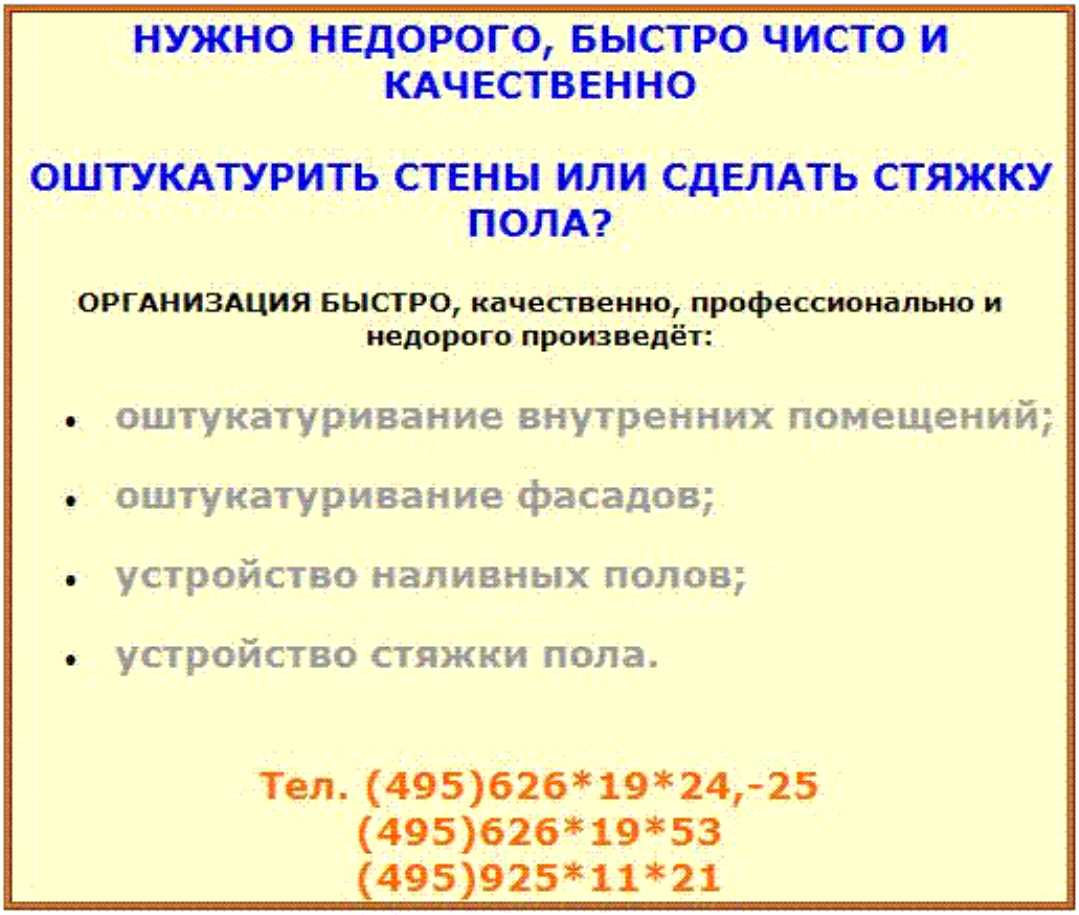
Political themes play an especially prominent role in today's online attacks because of their strong appeal to a wide audience. This threat continues to demonstrate a well established practice among today's attackers - tricking users into infecting themselves through the use of enticing messages based on current events. The one thing we can be certain of is that this particular incident is neither isolated, nor likely to be the last one we see.

Russian Spammers Are Waiting For Your Call

Spammers around the world continue to innovate new spam techniques to deliver their messages. This month's report noted that four percent of all spam originates from Russia. While Russian spam is not a new phenomenon, in the last few weeks an increase in Russian spam offering products and services has been observed. The primary action required for the recipients of these particular spam messages is to call a telephone or ICQ number. It is not uncommon for Russian spammers to use these numbers as their preferred method of contact.

One of the interesting points behind the attack is the simplicity of the localized services offered. For example, the spam emails included ads for everything from audio books to real estate, and from personalized accounting services to the installation of auto glass. For these types of services, it may be that maintaining a dedicated website can be costly and unnecessary. These spam emails also use text obfuscation by inserting unnecessary symbols between the numbers mentioned in these messages, which may be yet another attempt to evade spam filters.

From: Header Details Removed
To:
Cc:
Subject:



Translation:
Do you need Clean Fast and high-quality wall plastering or floor leveling service?

Our ORGANIZATION will do professionally cheaper and quicker following jobs:
• interior plastering;
• exterior plastering;
• floor levelling;
• floor foundations

Tel. (495) 626 * 19 * 24 -25
(495) 626 * 19 * 53
(495) 925 * 11 * 21

The Underground Path to Illegal Gambling in China

Macau is the only place in China where gambling is legal.* In order to gamble legally in China, a person would need to spend money on travel and accommodations to get there. Is there a way to avoid the hassle and expenditure of travelling to Macau for those who are interested in gambling? Well, it seems that spammers are offering a solution - gambling online, from the comfort of your home.

Symantec has recently observed what we believe to be the first instance of online casino and sports betting spam using the Chinese language. The layout of the message is very similar to what we frequently see in English-language casino spam. The message asks users to download a number of software packages and register an account. By registering an account, a user automatically becomes eligible for a random amount of free cash or bonus points.

With development of the growing casino business in Macau, and possibly an increased demand from remote locations, we may be witnessing a new trend in Chinese language spam - online gambling promotion. The example below includes the common spam attributes such as randomized "From" names and email addresses. Chinese characters in the "Subject" field are also randomly separated by symbols. Its corresponding promotion domain is registered with a Singaporean address; however, there's no physical address for contact to be found on the website.

The randomization observed in these messages is also commonly seen in English-language casino spam. So far, the volume of this spam type is not significant. However, we will be keeping a close eye on it to monitor changes in volume and technique.

Header Sample:

From: "khyci" <cjeovsjguqad@163sina1.[domain removed].com>

Subject: order Đ.Đ.Đ.Đ.88.00.Đ

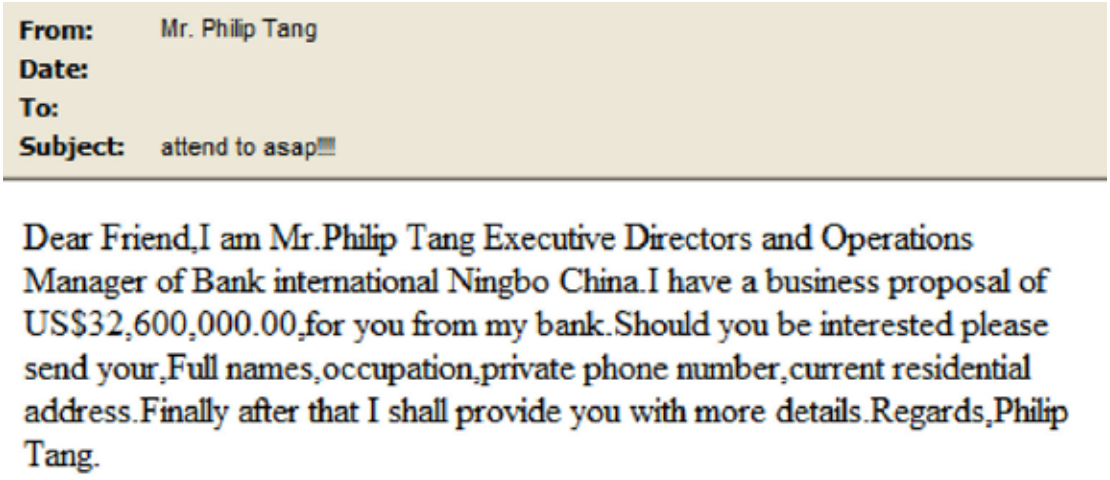
(Translation: Subject: order Regis.ter.Now.and.We'll.give.out.88.00.doll.ars.for.free)

*(State sanctioned lotteries are the only legal form of gambling in China, excluding Macau.)

Keeping the Focus on Nigerian Spam

In the February 2009 Symantec State of Spam Report, we have added another category of spam to those we closely monitor. Nigerian or 419 spam is named after the section of the Nigerian penal code dealing with fraud, and refers to spam email that typically alerts an end-user that they are entitled to a sum of money by way of lottery, a retired government official or a wealthy person that has passed away. In recent years Nigerian spam has evolved to include scam messages targeting non-African countries, news events and lottery-based scams. This spam attack is also sometimes referred to as advance fee fraud.

The characteristics of these scam messages vary but generally include an inordinate amount of capitalization, typos, incorrect English grammar and references to collecting and/or obtaining a sum of money. The general action required for the recipients of these spam messages is to reply to the email using an email address provided in the message body or header. Nigerian spam often uses legitimate services such as webmail to distribute this spam attack. In January 2009, approximately three percent of all spam messages could be categorized as Nigerian spam. A typical example of Nigerian spam is shown below.



From: Mr. Philip Tang
Date:
To:
Subject: attend to asap!!!

Dear Friend,I am Mr.Philip Tang Executive Directors and Operations Manager of Bank international Ningbo China.I have a business proposal of US$32,600,000.00,for you from my bank.Should you be interested please send your,Full names,occupation,private phone number,current residential address.Finally after that I shall provide you with more details.Regards,Philip Tang.

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*

- **Nigerian spam** is named after the section of the Nigerian penal code dealing with fraud, and refers to spam email that typically alerts an end user that they are entitled to a sum of money, by way of lottery, a retired government official, lottery, new job or a wealthy person that has passed away. *This is also sometimes referred to as advance fee fraud.*