



Confidence in a connected world.

The State of Spam

A Monthly Report – January 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

The new year is a time for resolutions; however, it is clear that as 2009 begins, spammers have not yet resolved to give up the spam war. Recent spam volumes indicate spam has slowly crept back up to 80 percent of their pre-McColo shutdown levels.

The following trends are highlighted in the January 2008 report:

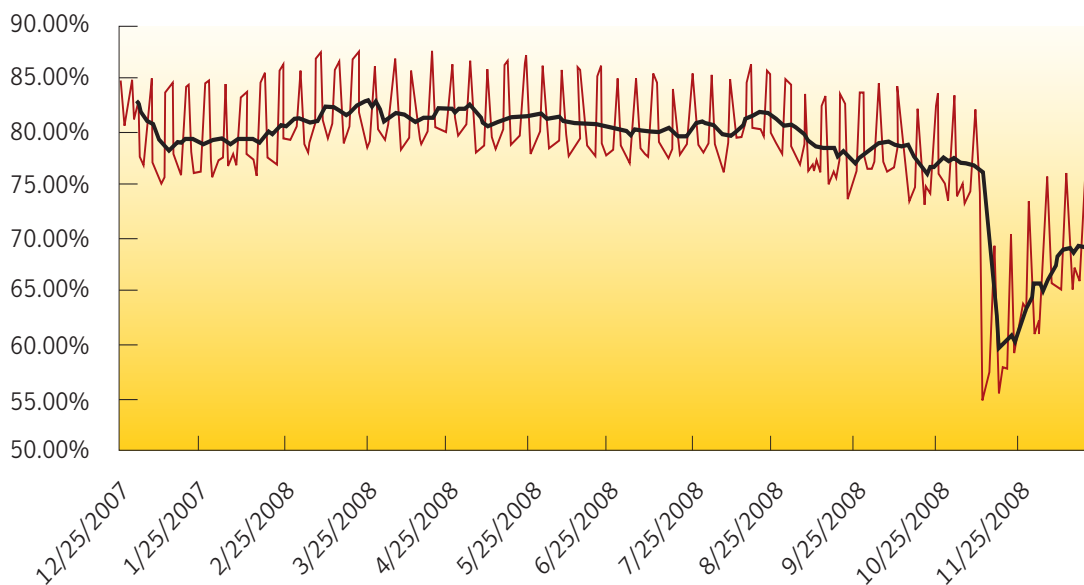
- **Memory of McColo Shutdown Fades as the Increase in Spam Volume continues in December**
- **A Spammer Sent You a Message**
- **Holiday Season Passes with Another E-card Spam Attack**
- **Spammers Continue to Piggyback on Legitimate Newsletters**
- **Spammers Use the Recession to Enter Your Inbox**
- **Spammers Aren't Finished with President-elect Obama Just Yet...**
- **URL Spam – A Special Investigation**
- **Phishing Messages Evolve as Webmail Phishing Comes Along**
- **New Year Brings New Fraud Attacks**
- **Holiday Spam 2008 Recap**
- **Spam Hall of Shame: Spammers Offering Meds Expand Their Product Range**

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.)

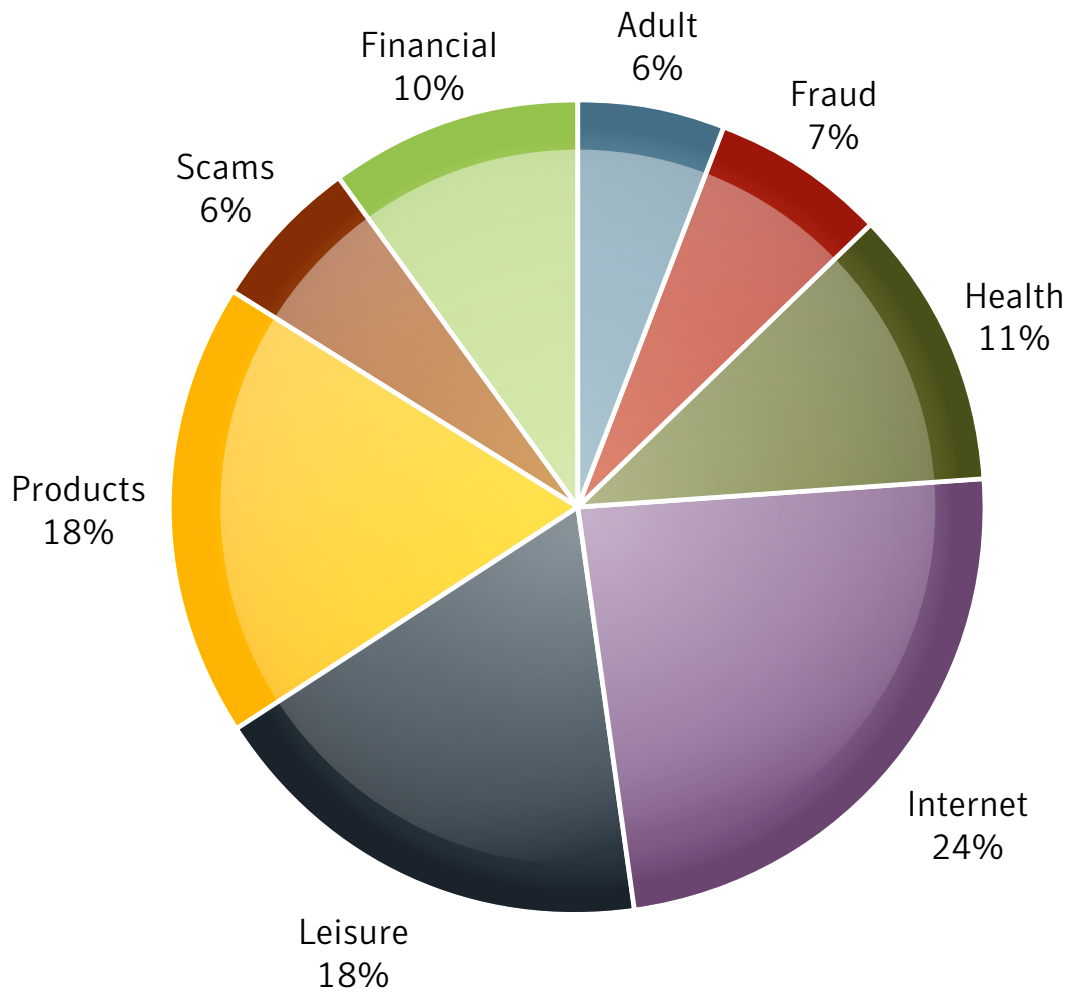


Global Spam Categories

Defined:

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

Global Category Count – Last 30 Days



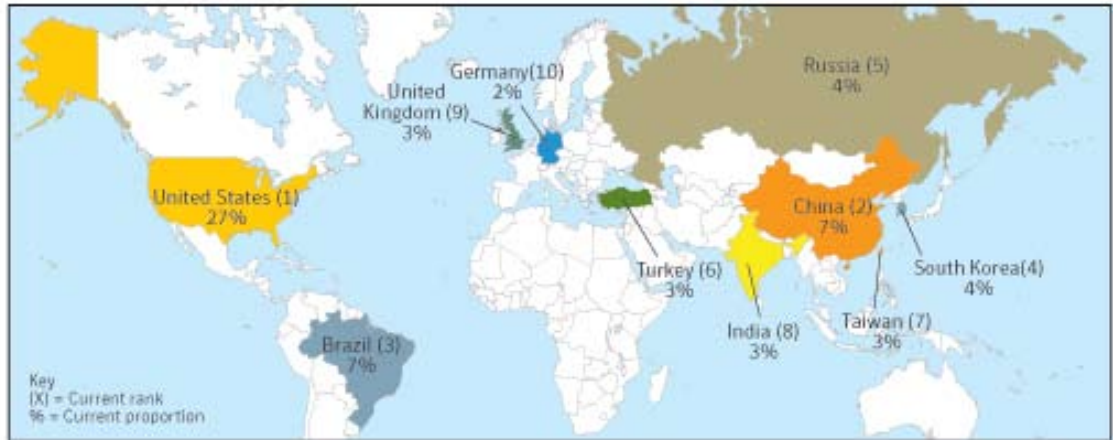
Category Definitions

- **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 misleading, 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:

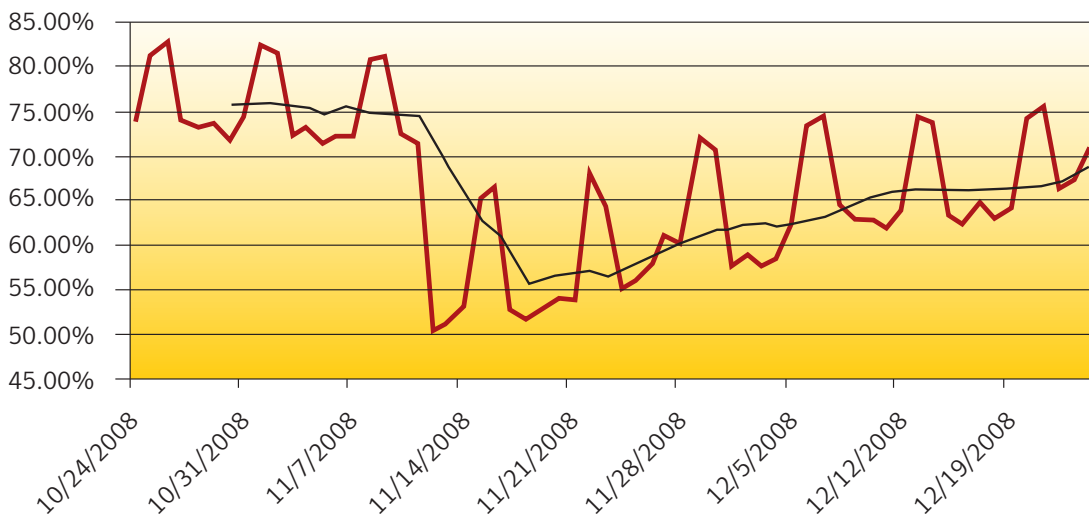
Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



Memory of McColo Shutdown Fades as the Increase in Spam Volumes continue in December

After the shutdown of McColo, which allegedly aided the distribution of about half of all Internet spam globally, spam volumes dropped dramatically. However, since mid-November, spam volumes have been slowly inching their way back up as old botnets are being brought back online, and new botnets are being created.

Spam volumes have gradually crept back up to 80 percent of their pre-McColo shutdown levels (when reviewing daily averages):



A Spammer Sent You a Message

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.

From: [Header Details Removed]
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: Direct message from [Header Details Removed]

It's so easy and cool, I love this thing!

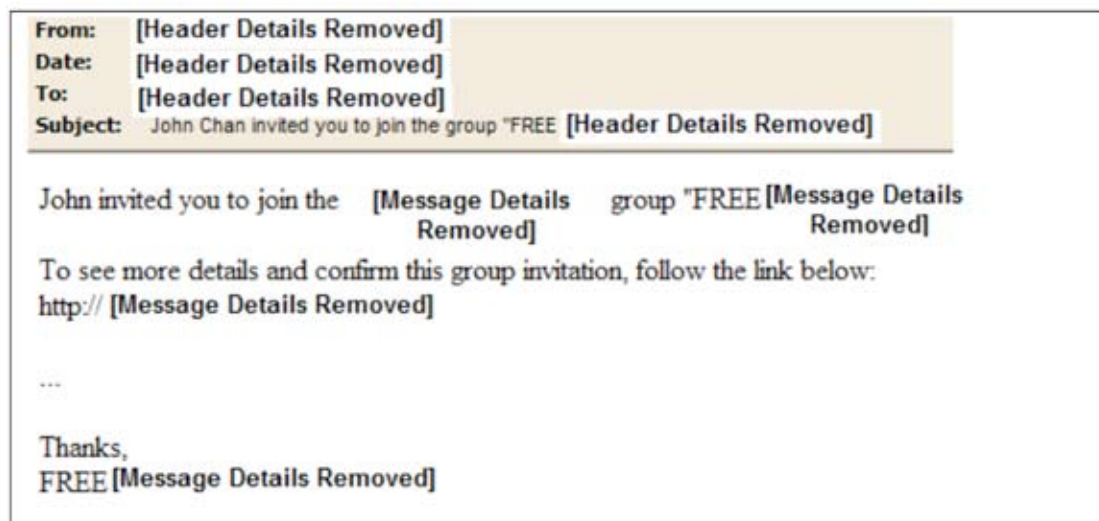
Visit: [Message Details Removed]

--

follow me at [http:// \[Message Details Removed\]](http://[Message Details Removed])
reply on the web at [http:// \[Message Details Removed\]](http://[Message Details Removed])
send me a direct message from your phone or IM: [code removed] your message here.
turn off these email notifications at: [http:// \[Message Details Removed\]](http://[Message Details Removed])

Spam Monthly Report, January 2009

In the second variation the user is invited to join a group on the social networking site. In this case the link in the email actually goes to a real group which was created on the social networking site by the spammer. The group then links to a free blogging site as an intermediary to redirect end users to the ultimate destination URL. So far many of the messages observed are using the same single social networking group. It may be because this was an experiment by the spammer or because the creation of multiple groups associated to multiple accounts could be too time-consuming.

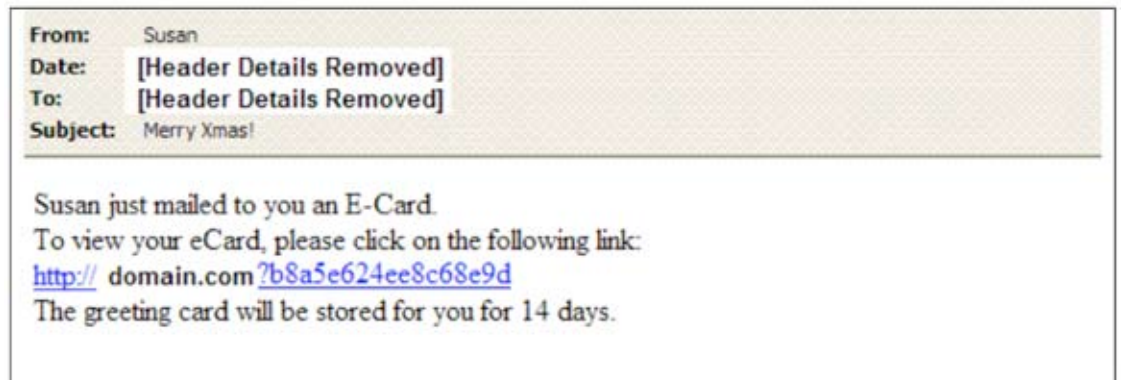


Once the user gets to the destination URL they are requested to fill out a form collecting personal information. This information can be sold on to marketing companies and / or used in future spam campaigns.

Symantec recommends that you do not accept any social networking invitations from names which are unfamiliar to you.

Holiday Season Passes with Another E-card Spam Attack

Greeting card spam that contains links to malware is not new. In August 2007, E-card spam accounted for approximately 15 percent of all spam attacks. While E-card spam has not returned to these levels, it is an attack that often re-emerges around high profile holidays. During the recent holiday season, E-card spam came to life with generic subject lines such as:



Each message contains a URL link to a “greeting card.” When clicked, the URL link delivers malware that can infect a recipient’s machine and allow it to become part of a botnet. Botnets can be responsible for both sending these spam messages, and also hosting the Web sites that cause malware to spread.

Spammers Continue to Piggy Back on Legitimate Newsletters

December 2008 saw a rise in the number of spam attacks which attempted to piggy back on legitimate email newsletters. This particular technique is an attempt by spammers to insert spam images within existing templates of legitimate newsletters and advertisements. The spam technique is designed to evade various antispam technologies as the majority of the data in the message appears to be legitimate data. This is also another example of how spammers attempt to hide behind the reputation of legitimate senders in order to deliver spam messages to recipients' inboxes.

The example below plays on The Food Network brand and the message itself contains a spammy advertisement for various pharmaceutical drugs. If the user clicked on any of the links within the message they would be taken to a URL site operated by a spammer which is being used to promote certain pharmaceutical products.

The image shows a screenshot of an email interface. At the top, the header information is as follows:

- From:** Network Newsletter
- Date:** [Header Details Removed]
- To:** [Header Details Removed]
- Subject:** [Header Details Removed] Get Ready for the New Year

Below the header is a red banner with the date "December 30, 2008" and a search bar. The main content area features the Food Network logo and a "Home" link. A large photograph of a dining table with various dishes and drinks is displayed. Below the photo is a white advertisement for pharmaceuticals with the text "BEST PRICE ON NET" and a red diagonal banner that says "WORLDWIDE SHIPPING". The advertisement lists five products with corresponding pill images:

- VIAGRA (blue pill)
- LEVITRA (orange pill)
- CIALIS (yellow pill)
- VIAGRA SOFT (blue pill)
- CIALIS SOFT (yellow pill)

Spammers Use the Recession to Enter Your Inbox

As the economic recession continues to impact the world, it is no surprise that spammers are still leveraging the state of the economy to target end users and deliver their spam messages. Some of the recent economy -related subject lines include:

Subject: Bailout Checks to be made available in less than 30 days
Subject: Recession Solution for Debt
Subject: As Seen On Tv: Recession Proof Way To Make Money
Subject: The Recession Proof Way To Make Money
Subject: Turn the bad economy into \$\$\$, in your pocket
Subject: I Found You a New Job.
Subject: Survive the Recession; earn 500 dollars or more a week!
Subject: I found you a new job [500+ a week]



What is interesting about these attacks is the different ways the economic situation is being used by spammers. Bogus work-from-home schemes are used along with survey spam, which both try to obtain personal information from end users. Economic spam related to the recession has been observed in a variety of languages, including Chinese.




We believe that spammers will continue their attempts to leverage the uncertain economic times to lure the more susceptible to these potentially malicious offers.

Spammers Aren't Finished with President-elect Obama Just Yet...

As Inauguration Day approaches, President-elect Obama's desk is full of important tasks. Among these tasks is the promise he made to his daughters to provide them with a puppy. Not wanting to leave this promise unexploited, spammers have jumped at the opportunity to use the prospective puppy in one of their survey spam attacks. The survey simply asks, "What kind of dog should Barack Obama get?"

From: Obamas new dog
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: Peter be rewarded for your opinion

[Peter, what kind of dog should Obama get.](#)



e-researchcenter.us.com

What kind of dog should Barack Obama get?

Vote! Get a **FREE** \$100 VISA gift card.
Participation required. See below for details.

GO

VOTE
DON'T MISS THIS ONE OFFER

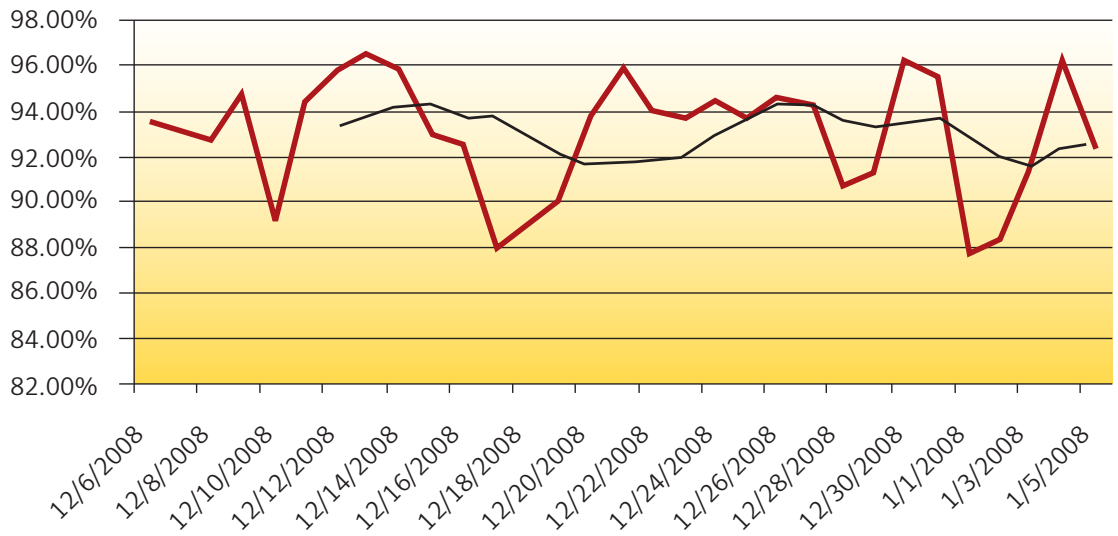
How is this possible?
Since e-researchcenter.us.com sponsors pay to be part of this program, it allows us to give our participants incredible gifts. You receive your gift once you complete the eligibility requirements.

President-elect Obama has been targeted by spammers in numerous ways including: his recent European tour, a special Obama presidential coin offer, and even a DVD which purportedly was a "Barackumentary." President-elect Obama has joined the ranks of high profile individuals and celebrities whose names and activities are used frequently by spammers to spread their wares.

URL Spam – A Special Investigation

ICANN stipulates that all domains must be connected to a registrar, and all applications for domain names must be submitted through a registrar. Today there are hundreds of thousands of Web sites registered. The process is simple and not very costly.

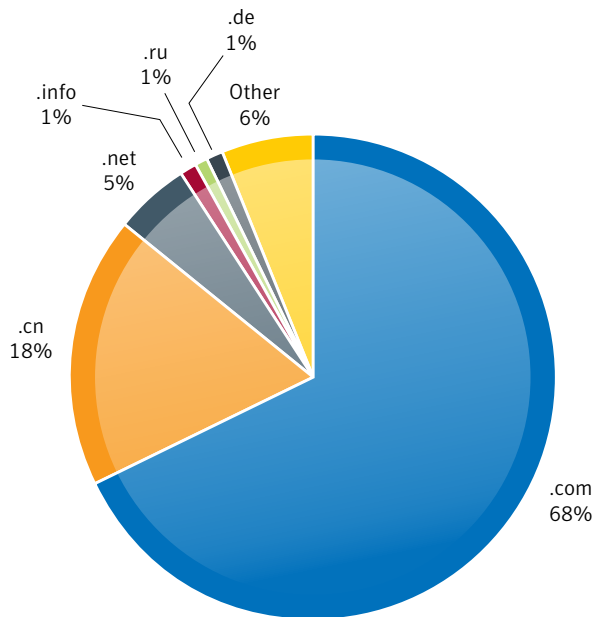
However, spammers can easily register domains, and it is often hard for registrars to distinguish between spammers and legitimate organizations and Web site developers. Spammers often rotate domains in their spam messages as they feel this tactic allows them to circumvent some antispam filters that depend on pattern matching to block the spam message. On average approximately 90 percent of all spam messages today contain some kind of a URL.



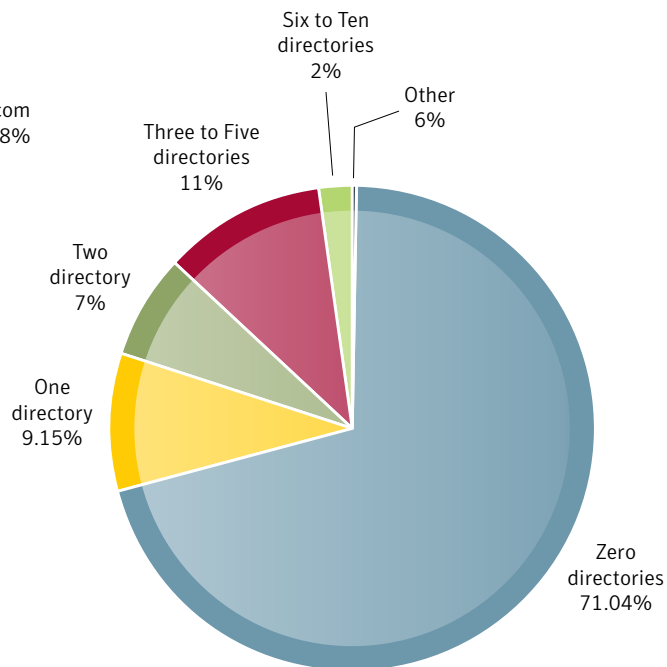
A top-level domain (TLD) is the part of a domain name that follows the final dot of any domain name. For example, in the domain name www.symantec.com, the TLD is com. A country code TLD (ccTLD) is a top-level domain generally reserved or used by a country or a dependent territory. A recent analysis conducted by Symantec showed that over the last 7 days 68 percent of all URLs in spam messages had a com TLD, 18 percent had a cn ccTLD which is reserved for China and 5 percent had a net TLD. Ru is the ccTLD for Russia and de is ccTLD for Germany. Spammers often rotate between TLDs to try and evade antispam filters.

Directories are often used to arrange or display certain files, and Symantec found that while 71 percent of URLs in spam messages had no directory, 2.4 percent had more than six directories. Similar to subdomains scammers often use many directories as the spammers try to create URLs that look like legitimate URLs.

URL TLD Distribution



URL Directories



Phishing Messages Evolve as Webmail Phishing Comes Along

Webmail phishing was first reported in early 2008, but it has recently gained a higher profile. The call to action or general purpose of the attack is to obtain webmail credentials such as passwords and contact list email addresses. A number of different scenarios have been employed by webmail phishers to try and secure this information and include:

Scenario 1

“We write to bring to your notice that we will be caring out some temporary maintenance on our service due to congestion in all email accounts and we are afraid that during this process email accounts of our customers will be deactivated; but just to avoid your email account from been deactivated and to enable your records remain in our database we advice you provide us with the below information or your email account will be suspended within 48 hours for security reasons.”

Scenario 2

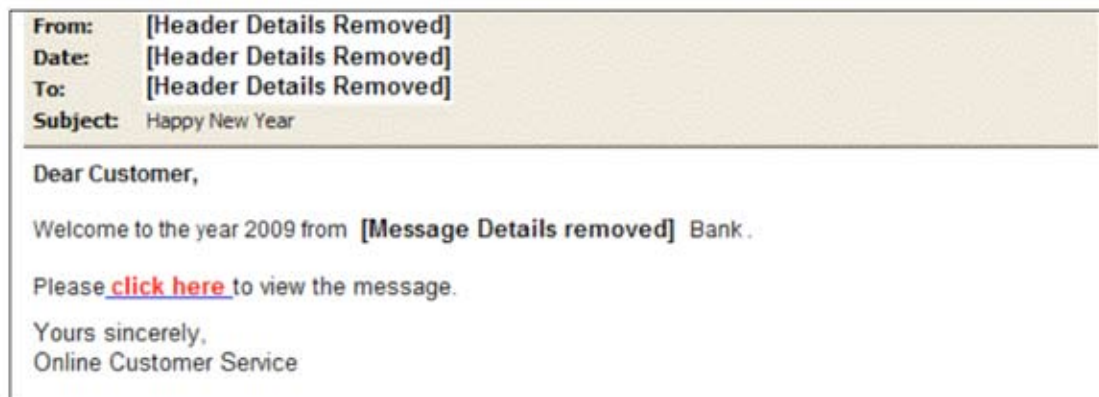
“Due to spam complaints of email users in our [Name Removed] webmail system, our investigation shows that your email address is compromised and is used to send out spam message in our [Name Removed] webmail system. As a result, your Username will be disabled if you do not send us the required information within 24hrs.” (sic)

As with other types of phishing messages, these are crafted to look like they are coming from a specific, legitimate organization and are then targeted towards members of that organization. One of the common features of webmail phishing is that the message is only in text. Unlike traditional phishing messages, the message does not contain a fraudulent URL link. The recipient is asked to use the address in the “Reply To” header or an email address in the message body to respond to the webmail phishing message.

It is clear that as long as the profit motive exists, the purveyors of phishing messages will continue to evolve and adapt their techniques to try and scam individuals and organizations.

New Year Brings New Fraud Attacks

2009 was a little more than a day old when one particular spammer decided to unleash a new fraud attack. Claiming to be a well-known banking institution, the spammer distributed a New Year's greeting with a catch. The message contained a link where another message could be viewed. When the URL link was clicked on, the recipient was asked to enter their "Personal ID OR 16 digit card number (not your credit card number) followed by your passcode and registration number in the boxes below" in order to receive an urgent warning about banking fraud. However this link was found to be fraudulent and any recipients who entered the requested information became a victim of this fraud attack where the consequences are unknown.



Holiday Spam 2008 Recap

There is nothing like a party to bring people together and the same could be said for holiday spam. The holidays have been used to peddle adult, leisure, finance, and meds products. The 419 spammers also celebrated with new spam attacks. Holiday spam attacks were not limited to the English language spam but also included non-English language spam which included subject lines such as "Subject: Cadeaux sexy pour Noel". Additional subject lines include:

Subject: New 2009 Models just arrived
Subject: Christmas safe online shopping starts here!
Subject: JOB OFFER!!! THIS HOLIDAY SEASON contact:
Subject: Winner Xmas Lotto Uk
Subject: Online Xmas Notification
Subject: Holiday Greeting Cards! No registration! No fees!
Subject: Send Holiday Hugs with a Vermont Teddy Bear

Subject: New 2009 Models just arrived
Subject: Christmas safe online shopping starts here!
Subject: JOB OFFER!!! THIS HOLIDAY SEASON contact:
Subject: Winner Xmas Lotto Uk
Subject: Online Xmas Notification
Subject: Holiday Greeting Cards! No registration! No fees!
Subject: Send Holiday Hugs with a Vermont Teddy Bear

**LOWER YOUR DEBT
UP TO 60%
THIS HOLIDAY SEASON**

**SPECIAL LIMITED
X-MAS SALE!**

GET EXTRA 50% PILLS WITH ALL ORDERS!

Canadian drugstore

Limited Xmas offer:
Extra 50% pills with every order

Spam Hall of Shame: Spammers Offering Meds Expand Their Product Range

Health spam currently accounts for approximately 11 percent of all spam messages. This spam category generally includes pharmaceutical products that could be obtained legally by visiting a pharmacy. It was with some surprise that another type of meds spam attack, which would typically attract the attention of law enforcement agencies, was observed in December 2008. The subject line for this spam attack included "Subject: LSD (BEST FOR HOME PARTY, ENJOY WITH BEST FRIENDS)." The plain text message instructed the recipient to respond via email to one of several free webmail accounts if they wished to take part in the offers.

From: [Header Details Removed]
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: LSD (BEST FOR HOME PARTY, ENJOY WITH BEST FRIENDS)

Online Store

Hello, we sell some drugs :

- Chub Drugs (GHB, Ketamine, and Rohypnol)
- Crack and Cocaine
- - MDMA (Ecstasy)
- Hallucinogens: LSD, Peyote, Psilocybin, and PCP
- Prescription and Over-the-Counter Medications (FREE SHIPPING !)
- Methylphenidate and Amphetamines (ADHD Medications) - BUY 2 GET 3 !
- Heroin (DISCOUNT 25% IF GET 0,5 Kilo)
- LSD (BEST FOR HOME PARTY, ENJOY WITH BEST FRIENDS)
- BUY BUNDLE MDMA + LSD and RECEIVE Methylphenidate for FREE !

Contact E-Mail: [Email Address Removed]