The State of Spam

A Monthly Report – March 2008

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Dave Forstrom
PR Contact
davidf@connectpr.com

Contributors

Kelly Conley
Manager
Symantec Security Response

Pavlo Prodanchuk
Sr. Security Response Technician
Symantec Security Response

Kevin X Yu
Security Response Lead
Symantec Security Response

Shravan Shashikant
Pr. Business Intelligence Analyst
Antispam Engineering

Frank Kuang
Security Response Technician
Symantec Security Response

Eric Lin
Sr. Security Response Technician
Symantec Security Response

Joseph Long
Security Response Lead
Symantec Security Response

Robert Vivas
Supervisor
Symantec Security Response

Samir Patil
Security Response Lead
Symantec Security Response

Monthly Spam Landscape

Overall spam volume stabilized in February for the second month in a row at 78.5% of all email. This is up from a 61% average for the first half of 2007. While tactics didn't stray much from tradition this past month, social engineering certainly seemed to drive the creativity among spammers—use of public figures, celebrities, events, and big brands.

Highlights from the report include:

- **U.S. Presidential Spam Race Heats Up:** First it was Ron Paul in October 2007, then Hillary Clinton in early February, and now amidst the heated race to the White House, spammers have added in the past couple weeks Mike Huckabee, Barack Obama, and John McCain to their campaigns.
- **Bogus Celebrity Videos the Latest Spam Bait:** It began with a bogus and malicious link to a Hillary Clinton campaign video, and now spammers are circulating similar video links for Michael Jackson, Heather Mills, and Indiana Jones.
- **Spammers Celebrate International Women's Day:** With social engineering a favorite tactic among spammers, there was no shortage of events and holidays to leverage this past month (i.e. the Super Bowl, Valentine's Day, President's Day), and International Women's Day is the latest celebratory target.
- **Spammers Ding Inboxes with Southwest Tickets:** It may not be the 'Ding' sound you hear occasionally on your desktop when a new airlines deal comes up, but spammers have hi-jacked the Southwest Airlines brand to offer free tickets to users.

Other notable items include:

- **Spam Spotlight: Regional Spam Trends APJ:**
  - Chinese Hit With Blizzards…of Spam
  - Chinese Sex Scandal is Spammer Dream
  - Pump and Dump, the Chinese Way

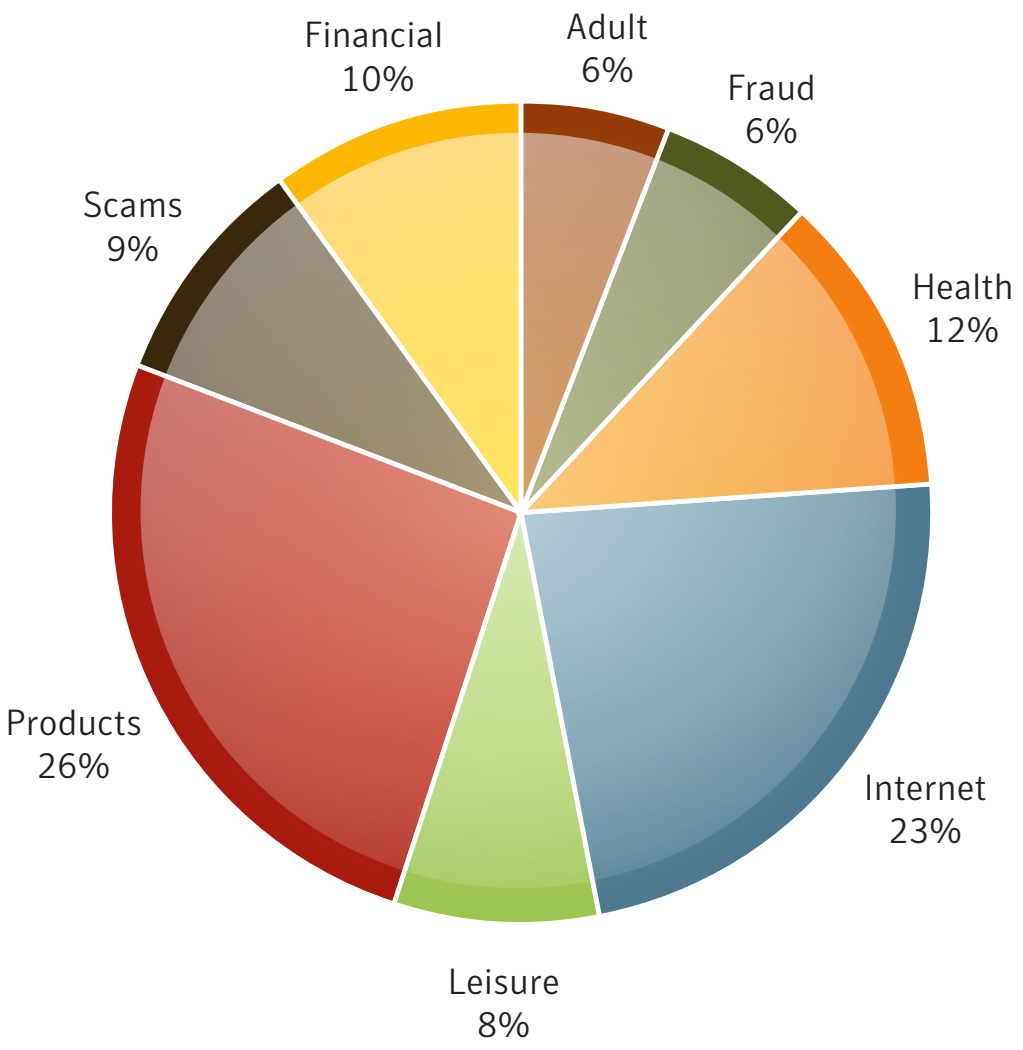
- **Spammers Hall of Shame:** Selling Burial Plots to Get Out From Being Buried

Global Spam Categories

Defined:

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

Global Category Count



Category Definitions

Products

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

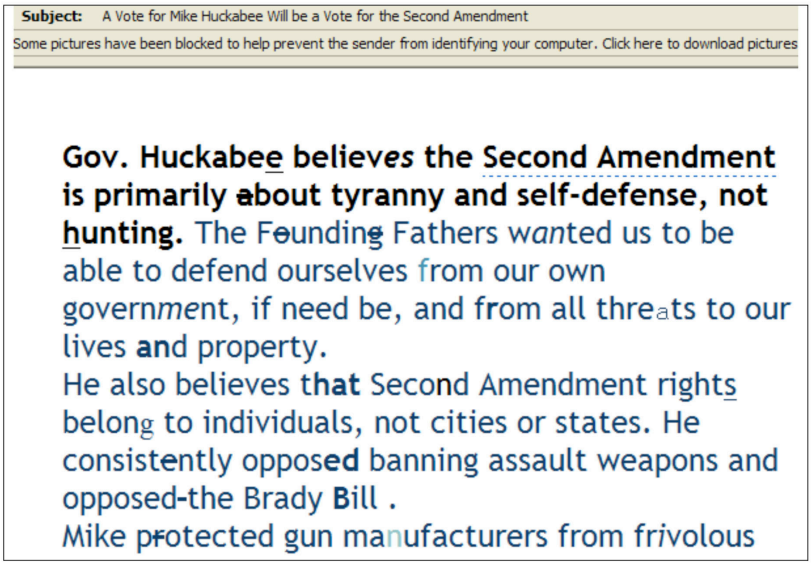
Email attacks specifically offering or advertising Internet or computer-related goods and services. Examples: web hosting, web design, spamware

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

U.S. Presidential Spam Race Heats Up

As the U.S. Presidential election continues to heat up, Symantec continues to monitor a growing surge in spam emails which make references to the presidential election candidates. In October 2007, Ron Paul emerged as the first candidate being leveraged by spammers. Paul was then followed last month by the first of the presidential frontrunners, when spammers began to circulate bogus links to Hillary Clinton videos cloaking a malicious Trojan. Since then, URLs containing Hillary Clinton's name have also been used in porn and Viagra spam. And now spammers have moved on to the remaining frontrunners. One spammer has cast a vote for Mike Huckabee, and Barack Obama and John McCain have had their names linked with 'portable dewrinkle machine' spam, meds spam, and get-rich-quick spam messages.



Bogus Celebrity Videos the Latest Spam Bait

Michael Jackson, Heather Mills, Indiana Jones, and Hillary Clinton have all been in the news recently. One wants to revive a pop career, one is in the middle of a divorce with a pop legend, one is a fictional character in a movie sequel, and one is a U.S. presidential election candidate. They all have one more thing in common too—spammers are leveraging their celebrity names to circulate bogus, and often malicious, links to videos.

The spam message entices users to open the message with Subject lines such as:

```
Subject: Hillary Clinton's campaign yesterday struggled to convince Democrats she can deliver
the strong wins
Subject: Hizer Mills showed in a court video about heavy life with Maccartni
Subject: Michael Jakson glued up a person a plaster
Subject: The first roller is presented to the film "Indiana Jons - 4"
Subject: Hillari Clinton stood up for daughter!!!
```

The message body is simple with a link to download a video relating to the particular celebrity such as :

Looking closer, the actual link is:

http://canotajetrilly.com/[REMOVED]/rdown.php?PNDcx”=id=3D

This link downloads a suspect file, “mpg.exe,” which is a Trojan downloader. This downloader downloads a file, inst241.exe, which is detected as Trojan.Srizbi. Trojan.Srizbi is really interesting for some unique features. Trojan.Srizbi driver (windbg48.sys) has two main functions: hides itself using a Rootkit and sends spam, but the thing that makes it really unique is the fact that its probably the first full-kernel malware spotted in the wild.

Once the Trojan is installed, it works without any user mode payload and does everything from kernel-mode, including sending spam. The Rootkit code is not new: the malicious driver attaches itself to \FileSystem\Ntfs to hide files on the local disk and also patches an SDT table to hide registry keys in the same manner other older rootkits did before. Also, the Trojan attempts to delete %System%\Minidump log files and seems to include a special routine to uninstall competitor rootkits, such as “wincom32.sys” and “ntio256.sys”.

Spammers Celebrate International Women's Day

Spammers using holidays to lure email users to their products and services has been a long-time favorite spam technique. The last month has seen social engineering around a variety of events and holidays—the Super Bowl, Valentine's Day, and President's Day—and now International Women's Day, which takes place on March 8th, has become the latest celebratory target for spammers.

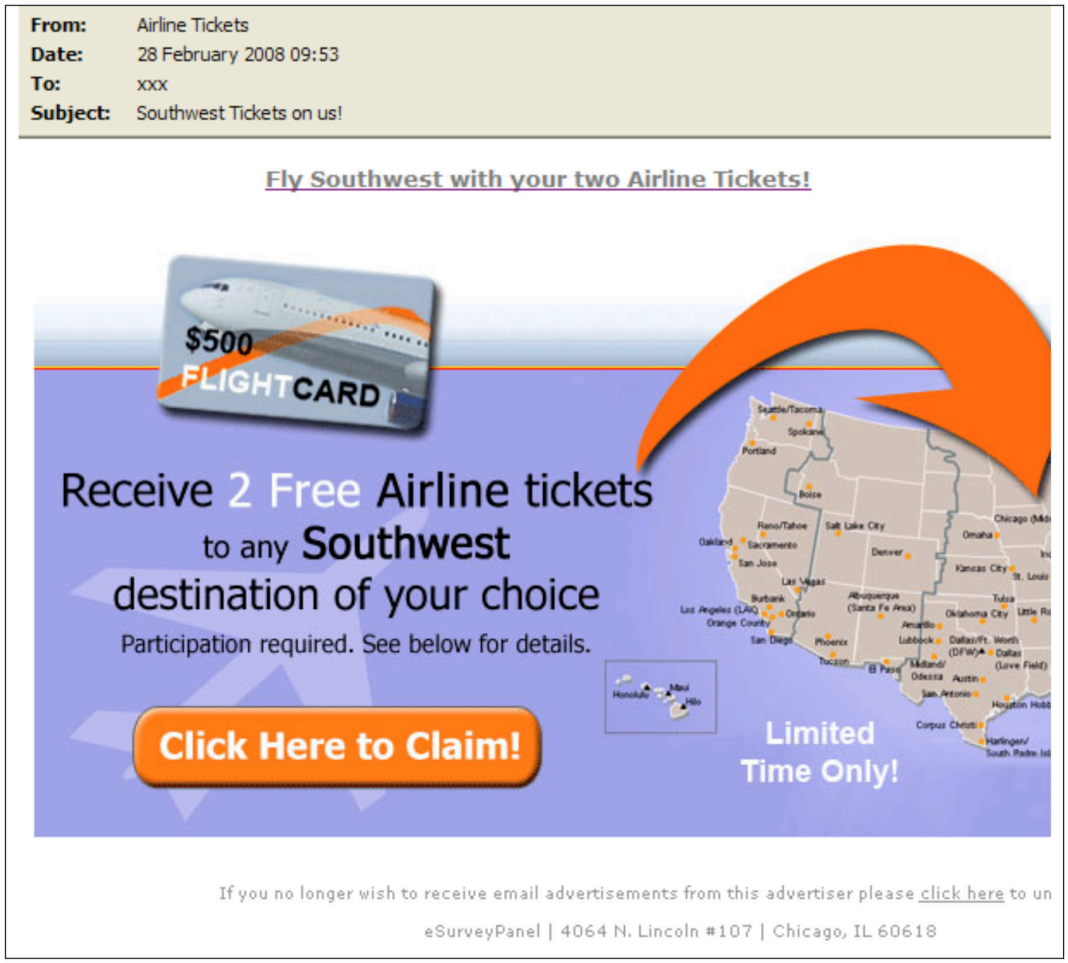
Spammers continue to use general holiday keywords and phrases in Subject lines and URLs to attract end users into clicking into the email message.

Some of the Subject lines used in Valentine's Day spam are listed below.

- Subject: Make it a special Valentine's Day
- Subject: Happy Comming Valentines
- Subject: Muaah, Valentines Day
- Subject: Hearts for you, Valentines
- Subject: Kisses for Valentines
- Subject: The Love, Valentines Day

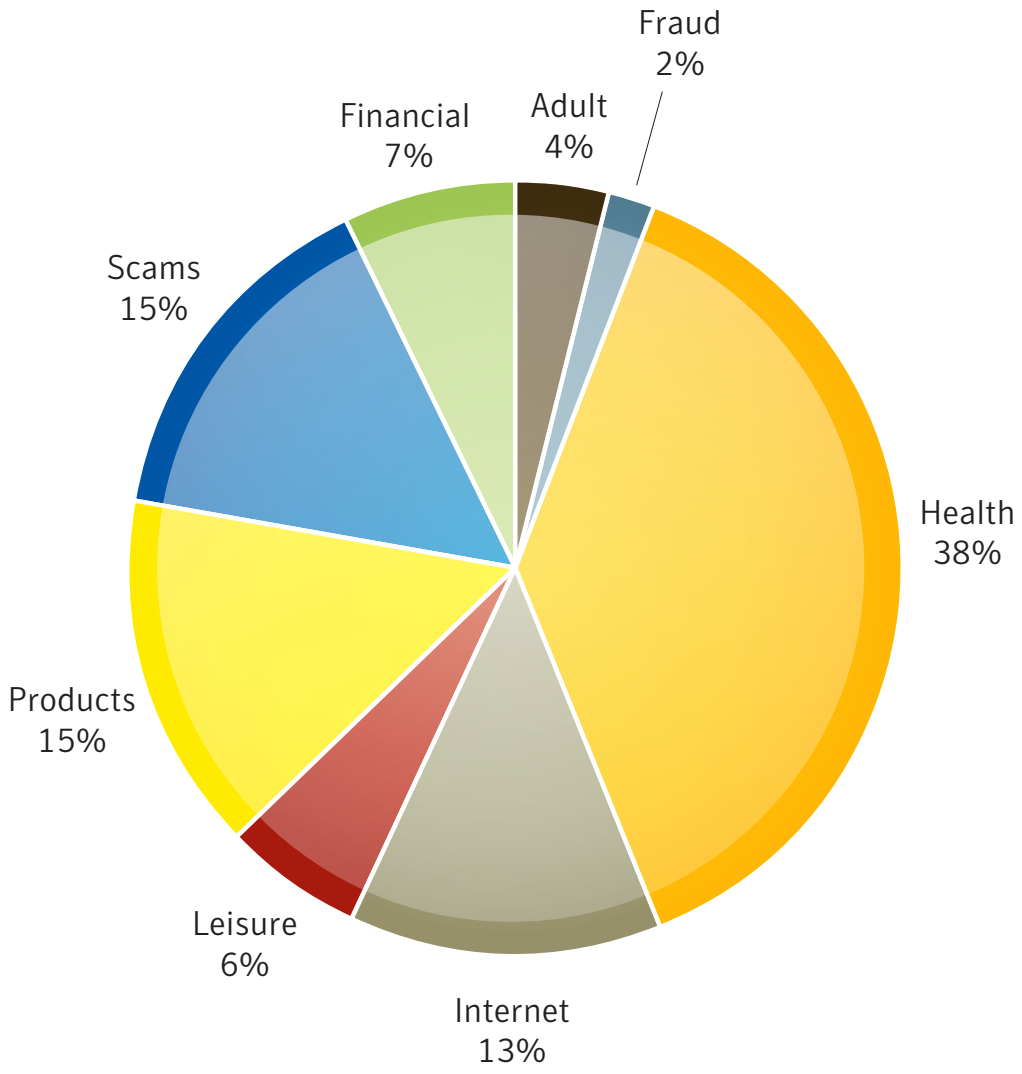
Spammers Ding Inboxes with Southwest Tickets

Using a standard brandjacking technique, spammers have recently sent out an email offering users two free Southwest Airlines tickets. In order to claim the tickets, the recipient must register their details, complete a survey, and possibly make some purchases from the spammer. The purpose of the spam email is to collect personal information from the recipient. The modus operandi used here is something that Symantec continues to see time and time again.



Spam spotlight: Regional spam trends APJ.

APJ Spam Categories Last 90 Days



A closer observation of spam tactics in APJ this past month revealed some interesting trends:

- Health spam, which includes pharmaceuticals, medical treatments, and herbal remedies, currently makes up 38% of all spam in APJ—that's a whopping 30% increase since November 2007 when the figures were last reported. Contrast this with the global percentage of health spam which is only 12%.
- The internet and product categories in APJ also differ significantly from the global percentages. Internet spam makes up 13% in APJ compared with 23% globally and product spam makes up 15% in APJ compared with 26% globally.
- Financial spam has also nosedived by 26% from November 2007 and now stands at 7%.

Chinese Hit with Blizzards...of Spam

Recent New Year snow storms brought misery to many and severely affected the public transportation system in China. Spammers who are always eager to exploit the most difficult of situations have found a way to benefit from this situation. Chinese language spam messages recently observed by Symantec, show a spam email which purports to be from a delivery company. According to the message, a package has not been delivered because of the snow storm. In order for the package to be delivered, the spam recipient is asked to reconfirm the delivery of the package by clicking on a link. This link brings the recipient to a personal blog, which is promoting general products and asks the recipient for personal information. As an old Chinese saying goes, “Prudence is the pledge of security.”

Chinese Celebrity Sex Scandal is Spammer Dream

Edison Chen, a Hong Kong-based movie star and pop idol, has recently been involved in a high profile sex scandal, where hundreds of private and nude photos featuring several female celebrities and himself were taken from his laptop and uploaded to the Internet. His predicament has attracted the attention of some Chinese spammers as they have realized that porn spam containing his name is a useful way to promote their product.

Some sample spam subject lines have included:

Subject: oax7y陳冠希事件(圖)yii

English translation: oax7y pictures of Edison Chen event yii

Subject: 6onfiiysbi陳i冠i希i最i希i迎i照ihtc

English translation: 6onfiiysbi Edison i Chen i new i sex i pictures ihtc

Subject: 更新囉~陳冠希艷照門無碼全集

English translation: updated Edison Chen pictures uncut full collection

Spammers always seek the most effective and efficient method to attract attention and encourage users to avail of their 'products.' By riding the wave of Edison Chen's sex scandal, spammers have found a way to reuse their techniques.

Pump and Dump, the Chinese Way

English language pump and dump stock spam has been on the spam landscape for some time now. The Chinese version has recently accelerated its growth as spammers realize the potential for this tactic.

There is one key difference between the English and Chinese versions. The English version of this spam attack encourages individuals to buy the stock, while the Chinese version encourages people to come together and form a group, collect money, and then buy the stock together.

Due to the recent celebrations for the Chinese New Year, this event features prominently in recent Subject lines, such as this one:

Subject: 关于: QQ地址 祝新年快乐！四季发财 - (Translation: About: QQ address: Happy New Year, May you be prosperous)

Most Chinese stock spam messages also supply the QQ group No. in the message. QQ is a form of instant messaging. This is one of the spammers' techniques to try and persuade users to join their group and prey upon the stock market. Novices.

好久没有联系了，股票做的好吗？

我找到了新浪答疑专家肖梦雷的博客: http://blog.sina.com.cn/u/1134319014Ð

他推荐的股票收益太高了，就是联系不上他。费了好多周折终于找到他的QQ群 54733152和33127064

（其他的群已满，要加就加这个吧）

English Translation:

I haven't contact with you for a long time. How's your stock?

I found a great blog,….

He recommend lots of excellent stock. Here is his QQ…

Spammers Hall of Shame

Over the course of many years, Symantec has seen spam "services" come and go that range from the extreme to the downright bizarre. This is another installation in what will be a continuing series of unique—sometimes humorous and others times simply inexplainable—shameful attempts by spammers to prey on their victims. Hence, we'll call it our "Spammers Hall of Shame."

Selling Burial Plots to Get Out From Being Buried by Your Home

As economic conditions have slowed in recent months, Symantec has observed a torrent of spam messages encouraging users to "refinance before its too late," "take out a mortgage for the lowest APR ever," or "this is the time to be the proud owner of your house." While the deluge of finance spam continues, spammers have also decided to diversify their sales portfolio to include the buying and selling of burial plots. Talk about an idea to get out from being buried, no pun intended. As the message indicates, the U.S. national average price for a burial plot in 1978 was $200 and this has risen to $4500 in 2008. "Get started today" – adverts say – "because tomorrow could be too late".