The State of Spam

A Monthly Report – October 2008

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Monthly Spam Landscape

During the previous two State of Spam Reports we noted an increase in the amount of spam messages containing URL links to malicious code. Now, with our October 2008 report, we highlight just how significant this trend is becoming. The increase began in May 2008 and continues to the present. During this period, there has also been an increase in email messages carrying malware payloads – not just links to malicious code. Spammers began to take a special interest in the economy beginning in October 2007, and this interest continues today as the economy dominates the news headlines. Evidence supports that overall spam levels have increased considerably since October 2007, and now averages 78 percent of all email.

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

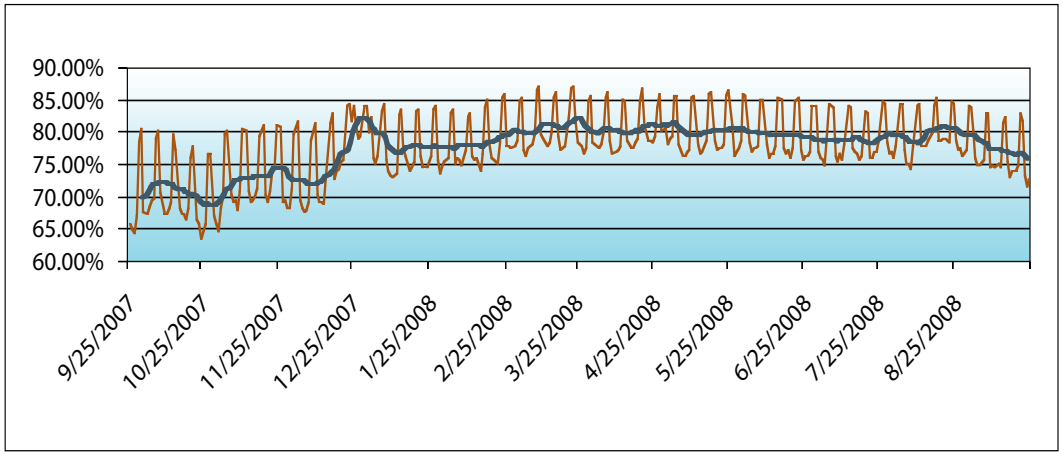
- **Spam Watch: Monitoring the Increasing Link Between Spam and Malware**
- **Zombie Activity Continues with the Help of their Voodoo Sorcerers (Spammers)**
- **Spammers Feed Off Economic Worries**
- **Spammers 'Rock the Vote' in the U.S. Presidential Election**
- **Spammers' Hall of Shame**

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



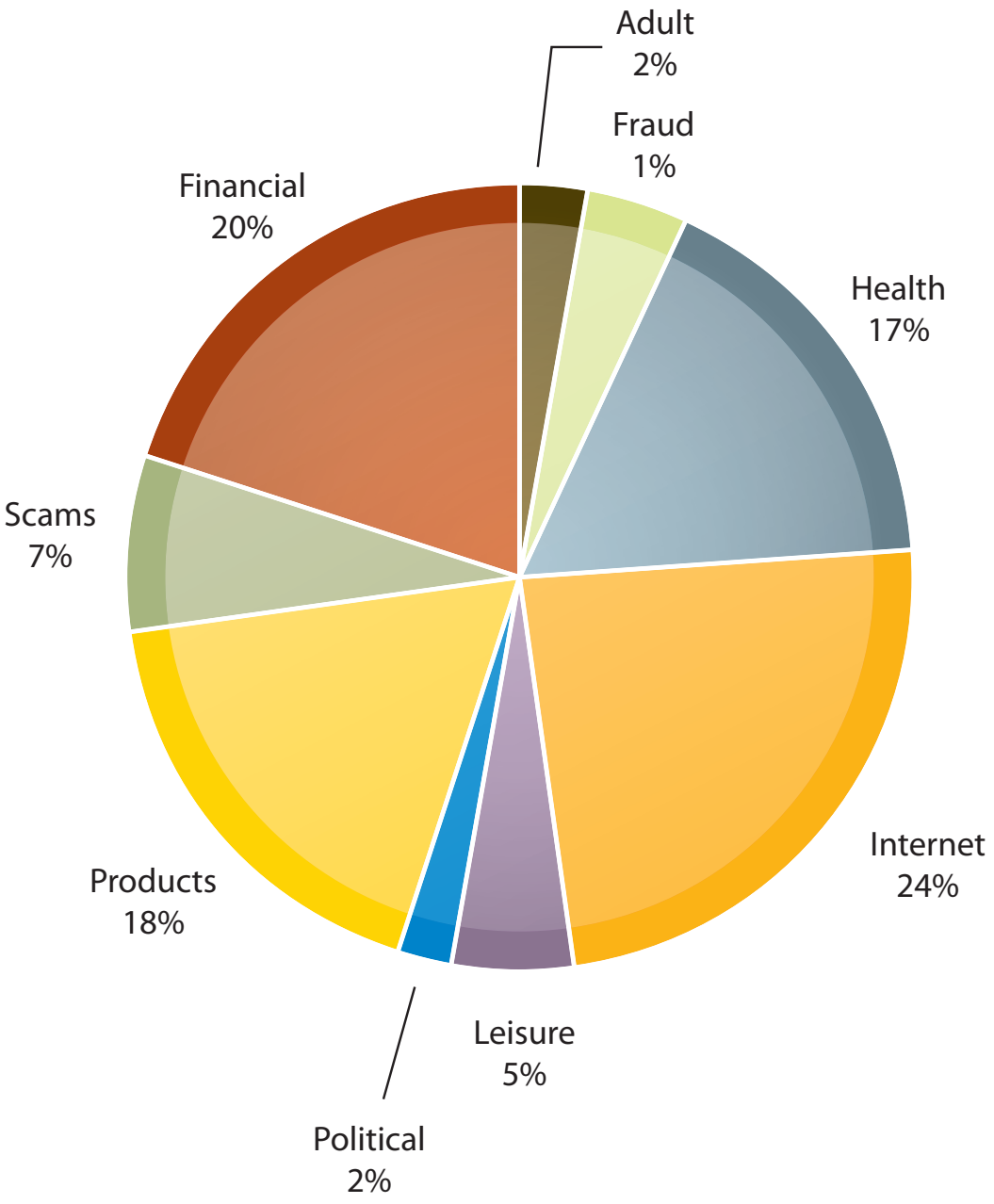
A trend line has been added to demonstrate a 7-day moving average.

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*

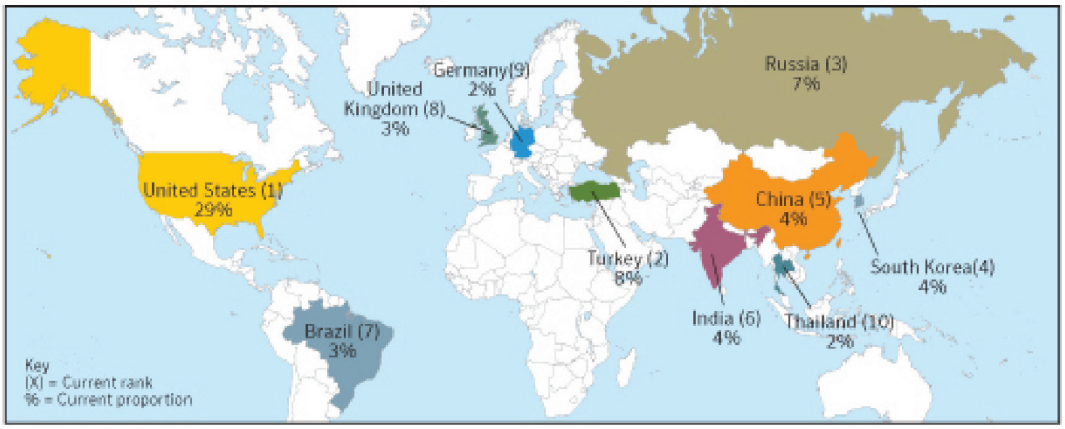
- **Spiritual E-mail attacks** with information pertaining to religious or spiritual evangelization and/or services. *Examples: psychics, astrology, organized religion, outreach*

- **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.



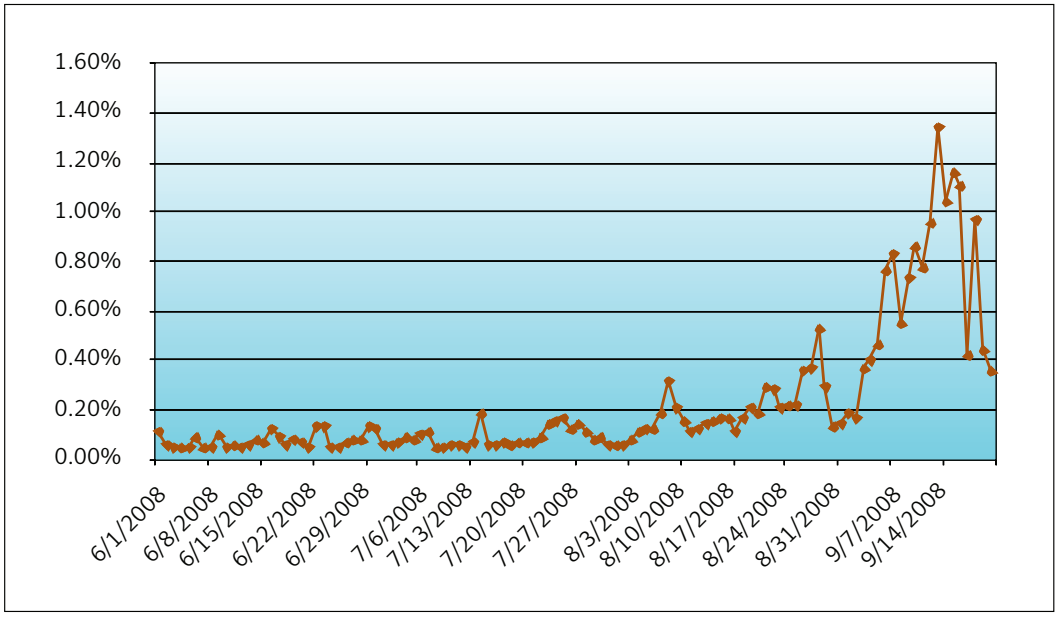
Spam Watch: Monitoring the Increasing Link Between Spam and Malware

The previous two State of Spam Reports for August and September have shown us a recent increase in the number of spam messages containing URL links to malicious code. Rather than simply promoting a spam product, these emails contain links to malware designed to infect other computers with viruses and Trojans. Following is an example of this type of attack.

The message contained the subject line, "The beginning of the Third World War". The URL in the message body included a spammy related domain cnnworld.org, an obvious play on the well-known U.S. television network. The URL directs individuals to a Web site where a legitimate looking style for CNN content is presented and the user is encouraged to download a video of the U.S. President.

Since June 2008, there has been an increase in the number of detected email messages carrying malicious payloads. The majority of this malware appeared in zip and RAR file payloads and were detected by antivirus filters. After zip and RAR files, the next most common payload vector for malware was those that were imbedded in the source code of email messages.

From June to mid September 2008, the percentage of malware detected in email messages had a dramatic increase from a tenth of a percent (0.1 percent) average in June 2008 to 1.2 percent in the middle of September 2008.

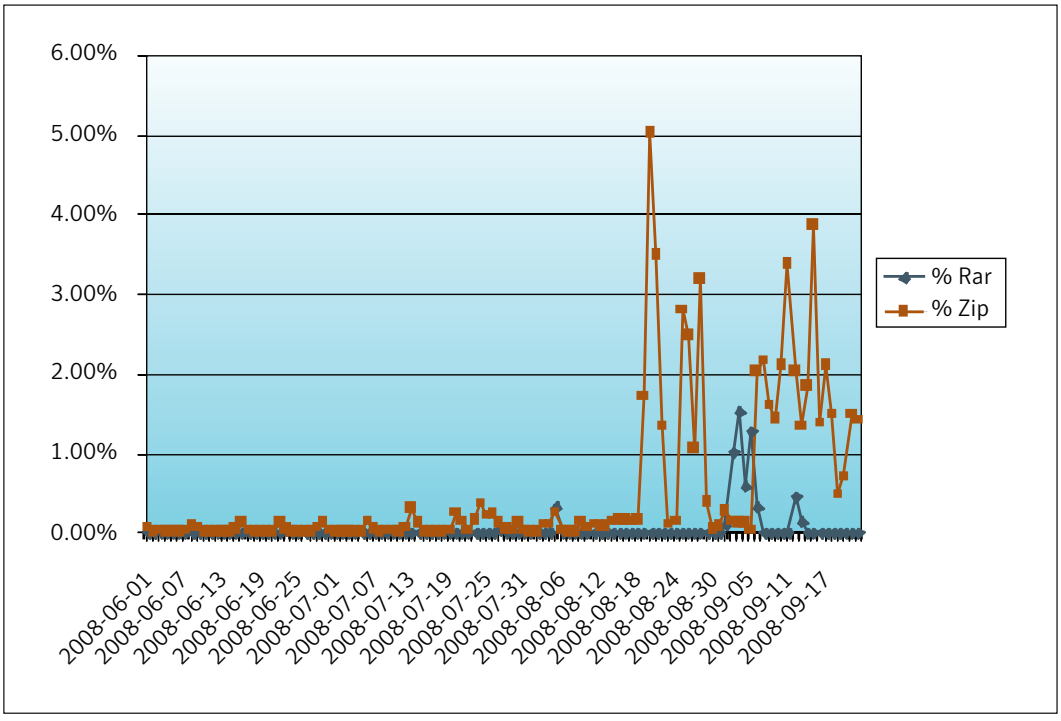


This is based on data that is retrieved from customers running antivirus software and have consented to return data. The total messages scanned includes legitimate and spam messages.

The top ten definitions detected by antivirus rules for this period were led by generic Trojan horse, Downloader and Infostealer definitions making up more than 30 percent of the malicious code detected. The generic Trojan horse definition, which identifies multiple Trojans that have similar qualities, led the detected programs with 13.4 percent of the messages identified. This was followed by Downloaders, malicious programs that can be used to download other malware, with 11.8 percent, and Infostealer with 11.1 percent. Infostealer is another generic definition which blocks programs that attempt to steal sensitive information from a user's computer. This following data is also based on data returned from the field, with definitions identified by antivirus software.

Name	Percent
Trojan Horse	13.4
Downloader	11.8
Infostealer	11.1
Trojan.Pandex	7.7
W32.IRCBot	6.8
Trojan.Goldun	4.9
W97M.Noifi!int	4.6
Backdoor.Paproxy	4
W32.SillyFDC	3.6

The correlation to zip and RAR files can be seen when viewing a spam stream in a lab environment for the period of June to mid September 2008. With data broken down for zip and RAR files detected, the patterns show that there is also an increase in these two file types.



The source of the email messages carrying the zip and malicious files appears to be varied. These were being sent out from compromised servers around the world, led by China, The Republic of Korea and the United States.

The Republic of Korea
United States
Thailand
Vietnam

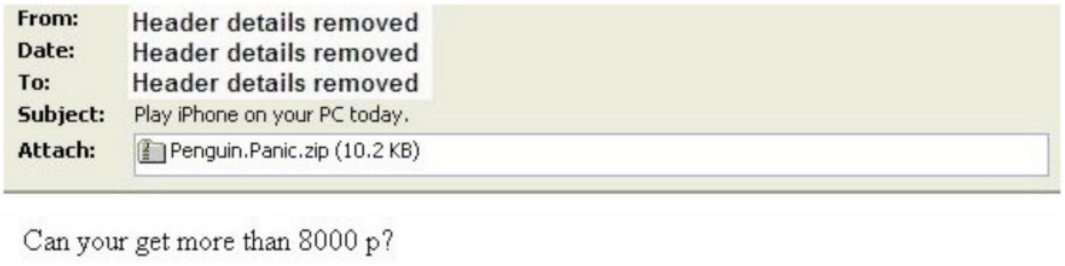
Reviewing one of the email messages carrying generic Infostealer malware a user will see an innocuous but potentially interesting subject:

"Play iPhone on your PC today"

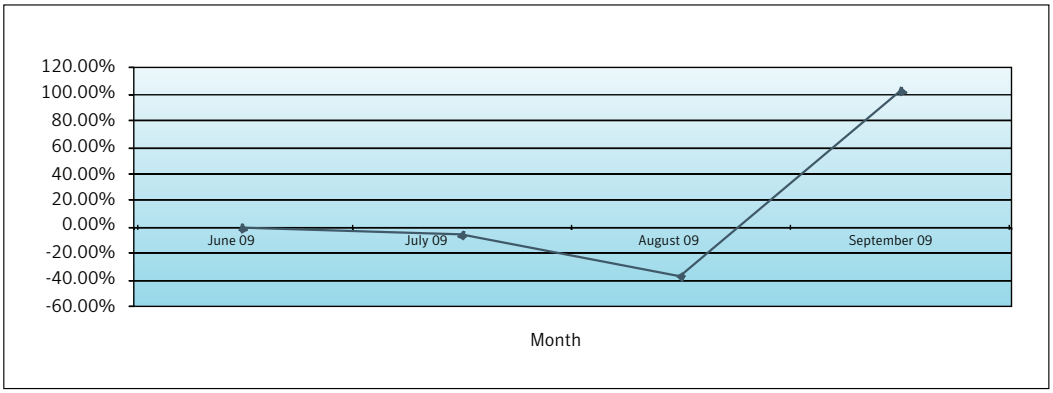
The body of the email simply says:

"Can your get more than 8000 p?"

Attached to the message is a zip file, "Penguin.Panic.zip," which the user would need to open to release the malware.



Zombie Activity Continues with the Help of their Voodoo Sorcerers (Spammers)
Zombie is a term given to a computer that has been compromised and is being used for various criminal related interests such as sending spam, hosting Web sites that advertise spam and acting as DNS servers for zombie hosts. In the past three months we've noticed an interesting trend with the number of active zombies and their presence around the world. In August of this year, when compared to July of this year, we noticed a drop in the number of zombies sending spam. As shown by the graph below this was a very noticeable 37 percent drop in the active zombie population. However, in September, we observed a 101 percent increase in the number of active zombies sending spam.



The top 10 countries hosting active zombie machines in this period are listed below:

Country	Percentage of Zombie Computers (Sep 08)
Turkey	12%
Brazil	9%
Russia	8%
United States	6%
India	6%
China	6%
Germany	5%
Argentina	4%
Poland	4%
Thailand	3%

For this period, the EMEA region was the leading source of all zombie IP addresses. Of the countries making up the EMEA region, Turkey was the top producing country. For the other regions the top producers were Brazil in Latin America, United States in North America and India in APJ.

We can get a better sense as to what countries are most responsible for the 101 percent increase in zombies sending spam by looking at the growth of zombies by country. Shown below are the 10 countries which showed the greatest increase in the number of zombies:

Country	Percentage Change from August to September 08
Korea, South	4236%
Kazakhstan	761%
Romania	607%
Saudi Arabia	555%
Vietnam	540%
Pakistan	454%
Turkey	310%
Iran	233%
China	229%
Morocco	155%

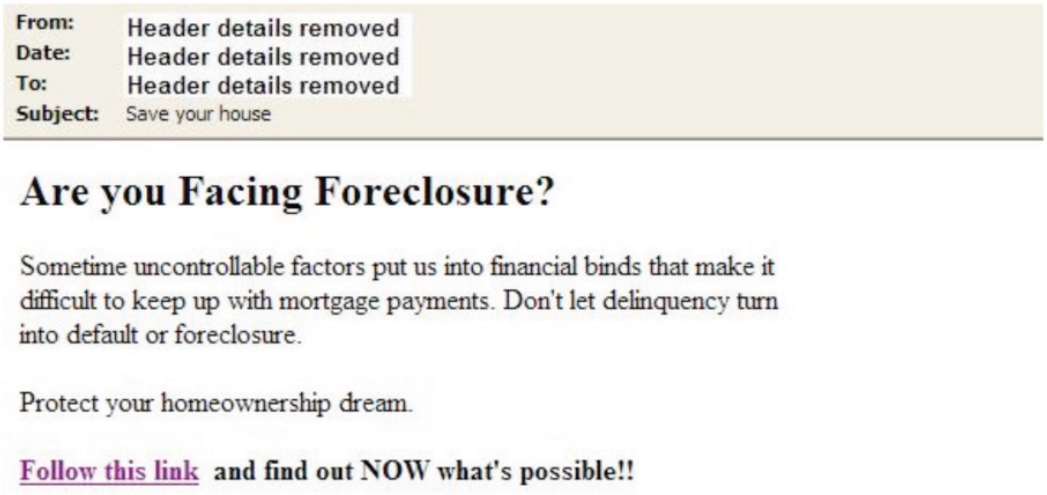
South Korea led the list with a 4236 percent increase in zombie machines. Interestingly, Turkey and China which figured in the top 10 list by number of zombies also hold a place in this list by showing a 310 percent and 229 percent increase respectively over the past month. Other countries such as Vietnam, Romania and Saudi Arabia with high zombie footprints also showed substantial increases during the past month.

While it's difficult to determine an exact reason for the increase, it does coincide with the increase in email messages carrying links to downloadable exploits which were characterized by their use of sensational news headlines. It also coincides with an increase in email messages carrying attached viruses in the form of zip and RAR files. It's quite possible that those attacks have had some impact on the trends that we see here, especially when looking at the geography of the virus attacks versus the zombie data. There are similar increases in certain countries on both accounts.

Spammers Feed Off Economic Worries
We continue to see spammers leveraging the housing market downturn and the general economic instability in the U.S. as a vehicle to promote their spam attacks. Leveraging the intense interest in these current events, spammers hope to collect personal information from their targets. As news of the economy continues to dominate headlines, it is apparent that spammers will continue to use this angle to try and exploit email users.

Recent subject lines for this type of spam include:

Subject: Save your house
Subject: Don't go into foreclosure
Subject: In fear of foreclosure


From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Save your house

Are you Facing Foreclosure?

Sometime uncontrollable factors put us into financial binds that make it difficult to keep up with mortgage payments. Don't let delinquency turn into default or foreclosure.

Protect your homeownership dream.

Follow this link and find out NOW what's possible!!

Spammers 'Rock the Vote' in the U.S. Presidential Election
As the November 4th U.S. presidential election draws near, spammers are leveraging the interest and scrutiny of candidates in their attacks. During August and September 2008, Symantec noted that the activities of the candidates were being used to spread malware. In January 2008, Symantec reported presidential polling scams promising gift cards and t-shirts in exchange for opinions on the election. During September 2008, we continued to see this scam. Recent subject lines for this scam have included:

Subject: Who will win the 2008 presidential election?
Subject: Vote - Is Obama ready to lead?
Subject: Are you voting for Obama/Biden or McCain/Palin?

Spammers' Hall of Shame

During the past several years, Symantec has seen spam "services" come and go that range from the extreme to the downright bizarre. This is another installation in a series of our reports on unique attempts by spammers to prey on their victims through methods that are sometimes humorous and others times simply unexplainable.

In September 2008, Symantec observed a particular spam trend in which spammers offered a device that they claimed would allow the user to see through clothes. According to the spammers, "This is the most important purchase of all my life. Everyone can be 'Undressed'!!!"
The purpose of this spam message was to obtain personal information from the recipient by promote the product.

From: Header details removed
Date: Header details removed
To: Header details removed
Subject: dotecbabed gini1987 rines1989 qehed8 coq1990

From now on you have something that no one among all the human beings has. A spy-device that lets you watch trough the clothes. It is a secret technology, which has no analogues.

Visit site: http:// **Message details removed**