Monthly Spam Landscape

September saw PDF, Image, and Ecard spam fall further off the radar, while overall spam levels continue to inch upwards increasing by 1% to 70% of all email traffic. Spammers also took a special interest in the U.S. housing market, capitalizing on news about the U.S. housing slump and the recent interest rate cut.

Highlights from this month included:

• **Spam Levels Continue to Inch Upwards.** Overall spam levels at the SMTP layer in September increased slightly to average 70% of total email. This compared with 69% of total email in August.

• **Image Spam Fades Further.** Image spam, which has recently fallen out of favor with spammers, faded even further in September and averaged 7% of total spam. This compared with 10% of total spam in August. (See Page 5)

• **Text- and HTML-based Attacks Pick Up the Slack.** While image spam is declining, text-based attacks are still very much in the wild:
  - Job Seekers Wanted……by Spammers
  - Reusing URLs and Common Brands Linked in Spam Messages
  - Format of Geocities URLs Used in Spam Continues and Diversifies
  - Use of Javascript Comments to Obfuscate URLs
  - Chinese Electronic Product Spam Through eBay

• **Spammers Feed Off Housing Crisis.** The recent discussion over interest rate cuts and weakness in the U.S. housing market does not go unnoticed by some spammers. (See Page 6)

• **Spam spotlight: Regional spam trends EMEA.**

Percentages of Email 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 email detected at the network layer.

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 (90 Days)

- Financial: 13%
- Adult: 7%
- Fraud: 3%
- Health: 12%
- Internet: 19%
- Leisure: 6%
- Products: 26%
- Scams: 10%
Category Definitions

• **Product 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 misleading, 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

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

• **Other Emails attacks** not pertaining to any other category.
Regions of Origin

Defined:
Region of origin represents the percentage of messages reported coming from each of the following regions: North America, South America, Europe, Australia/Oceania, Asia and Africa.
Percent Image 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 email detected at the network layer.

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

Spammers Feed Off Housing Crisis
There has been much talk of late about the slowdown in the U.S. housing market and the recent interest rate cut by the U.S. Federal Reserve. The uncertainty in the housing market has not been ignored by spammers. Recently, Symantec has observed a plethora of spam messages which are trying to tap into the market uncertainty. The spam messages range from refinancing deals to offers on houses to asking users if the "Equity" in their home is being used. Subject lines include:

- Subject: Pay your house off in 5-7 years
- Subject: Looking to sell your house fast?
- Subject: I want to buy your house
- Subject: We Buy Houses
- Subject: Equity in your house been used?
- Subject: Get the dough out of your house

While leveraging peoples’ fears about the housing market, spammers evaluate whether the recipient is eligible for one of these ‘offers.’ During the evaluation process, the spammer collects a large amount of personal information about the user such as name, address, email address, telephone number, etc. This is just another example of how spammers are using current news events to target individuals with their spam wares.
Job Seekers Wanted......By Spammers

“Work at home” spam messages have long been a stable message for spammers. These spam messages promise high wages for minimal effort- the prerequisites for some employees. The messages take the form of a job recruitment email. Legitimate recruitment message are common these days as many recruiters use online resources to find new employees. This month, Symantec observed one particular “Work at home” spam attack which comprised of over 100 million spam messages.
Reusing URLS and Common Brands Linked in Spam Messages

What do the following products and services have in common? Black Visa cards, Universal Makeovers, History Channel magazine subscriptions, and Dominos pizza. These products and services can be linked by recent spam attacks. The spam messages “provide” gift cards for these products and services if the recipient completes a survey. The interesting thing about these spam messages is that the spammers are consistently reusing the same spammy URL links while offering gift cards from well known brands. The technique of reusing URLs has previously been observed by Symantec, but the rate at which spammers are reusing URLs has become particularly blatant in recent times. April saw spammers using a particular URL to offer Dominos pizza gift cards and then in September, Symantec saw spammers using the same URL to offer History channel magazine subscription gift cards. Symantec has observed similar techniques used in Wallmart- and Target-related gift card spam.
Format of Geocities URLs Used in Spam Continues and Diversifies

Geocities offers users among other things an opportunity to build free Websites. Symantec has previously observed that spammers have sent spam emails with links to Geocities URLs. While spammers continue to use Geocities URL links of the form geocities.com/abcd38/ in their spam emails, Symantec has recently observed spammers using URLs of the form geocities.com/\abcv98/ ///. Notice the extra forward and back slashes around the folder name. While the change is very subtle, it is another example of how spammers are testing new techniques to try and evade antispam filters.

Use of Javascript Comments to Obfuscate URLs

During recent months when spammers were using ‘cn’ domains in their messages, Symantec saw a constant stream of medication spam emails using broken URLs. Spammers have long obfuscated URLs by using HTML tags in the middle of the link, such as <b> and <div>. When viewed in an HTML email, the URL looks normal to the end user and the URL is clickable. This month, JavaScript comments have been added and an attack of 400,000 messages was observed in a one-week period.

Raw html:

```html
<HTML>
<BODY>
<P><DIV>type parity fluffy</DIV></P>
<DIV><FONT face="Nice<y ghyl!" ariel" n e r t piz" ariel" 583Rg;sy in cre" odj" ariel" yma" se e qRA19h>|y|/wtdakj</FONT> ur p sizer|qPPbG| in the|vntqe| ma|<B r>P|b|=t+RykGg|=t+<G ab>f we|l+KyGOD|e|=t+trua|ks</DIV>
<P><DIV><b><font size="5" gr" h" anm" b</b>|g|t qhy|m.co</DIV></P>
</BODY></HTML>
```

What the end user sees:
Chinese Electronic Product Spam through eBay

This is not a phishing attack but a straightforward product spam. The code from a legitimate eBay message has been taken in order to make the email appear as though it’s coming through eBay. Even from the salutation alone, “Dear Friend,” this is an obvious spam.

Spam Spotlight: Regional Spam Trends EMEA

Overall spam trends in EMEA region have remained pretty consistent with trends observed in other regions. Symantec has, however, previously observed that spam attacks are more routinely being translated into languages apart from English. Some of the more high profile spam attacks by language are profiled below.
Adult Spam Plagues French Language Spam

The subject and message content are often fully translated into French. Subject lines for this spam messages have included:

| Pas de frais de souscription. Vidéo adulte sur demande. |
| Payez seulement pour ce que vous visionnez. Films adultes sur demande. |
| Pay-per-view adulte |
| Pay-per-view adulte pour l'ordinateur. Pas de souscription. |
| Pay-per-view adulte. Tout en HD sur votre ordinateur. |
| Photos sous-marines, Découverte bancaire, Meilleures universités. |
| Pré-visionnement de 15 minutes sur tous les films adultes |

Des milliers de vidéos adultes sur demande

One interesting thing to note is that the URL in the message body is often used previously in English language spam. Messages are of the form:

From: xoooo
To: xoooo
Subject: Des milliers de vidéos adultes sur demande

Pré-visionnez des close-ups des stars porno les plus fumantes.
La plus grande sélection de titres pay-per-view en HD
Pas de frais de souscription mensuelle!
http://xoooo.com/video
Portuguese Language is Added to Weight Loss Spam

The subject lines for this spam have included:

| imagine emagrecer dormindo 3  |
| Perdendo peso rapidamente   |
| revolucionario emagrecendo dormindo  |
| emagrecer dormindo 4         |

The interesting thing about this spam attack is that spammers have also set up dedicated Portuguese language URLs to include in their spam messages.

From: xxxxx
To: xxxx
Subject: O que é Sonodiet??

Sonodiet é um poderoso emagrecedor que atua durante o sono

Vários prometem mais apenas um cumpre! Visitem nossa Loja online e vejam mais informações e não vá mais perder o sono por excesso de peso durma e fique em forma naturalmente.

Sonodiet não tem contra indicações, é um produto 100% natural faz vo perder peso e ajuda ficar muito mais disposto

acesso nosso site abaxo

In Italy, Germany, and Spain Spammers Continue to Gamble on Casino Spam

The subject lines for this spam have included:

Dit is een prachtig aanbod
400 in bonus di benvenuto!
Depositate 100 e giocate con ben 400

From: xxx
To: xxx
Subject: Dit is een prachtig aanbod

Voel de unieke opwindig van hetspelen bij Europas beste on-line casinoâ€™ en ontvang â¬ 400 GRATIS als u lid wordt!

De eerste 4 keer dat u stort ontvangt u tot â¬ 100 in VIP spelbonussen voor elke storting. Wat een fantastisch aanbod, recht uit het hart van Europaâ€™s gokliden!

Dit is een prachtig aanbod, helemaal wanneer je ziet wat Euro VIP Casino nog meer te bieden heeft:

- meer dan 100 plezierspellen, realistische graphics
- de best beveiligde en up-to-date programmatur
- professioneel ondersteunend personeel om u te helpen bij wat u ook maar nodig mocht hebben, op elk moment van de dag en nacht!

Bezoek Euro VIP Casino en zie zelf het verschil.
Spammers See Opportune Time to Use Russian Language Watch Spam

Other Russian spam attacks observed recently have included novel Russian resume spam and Russian phishing attacks.

Novel Russian Resume Spam

Times are hard. We blocked over 12,000 copies of this Russian email in a four-day period. The content of the email is the curriculum vitae of an economics graduate looking for a job.
Russian Phishing

Here is a recent Russian phishing attack which consisted of over 10,000 email messages in one day.