Spam made up 92.51 percent of all messages in August, compared with 91.89 percent in July. In our July 2010 report, the highlight was the increase in malware spam. After taking a one-month hiatus, the attack has returned to the forefront of the spam threat landscape as .zip attachment in the September 2010 State of Spam and Phishing Report. Malware spam more than tripled in volume, and .zip attachment spam saw a four-fold increase month-over-month. In addition to the .zip attachment, there was a wave of .html attachments with malicious JavaScript.

With respect to origin of spam, the EMEA region continued to decline in August, sending 43.17 percent of spam. This is down over 5 percentage points since marking a high of 48.97 percent in June. North America region took up that slack by sending 25.78 percent of spam in August, compared with 20.49 percent in June. Latin America and APJ regions remained relatively flat over the same time period.

Phishing messages overall increased by 11 percent in July. The boost was primarily due to an increase in automated toolkit attacks. Phishing websites created by automated toolkits increased by 92 percent. Unique URLs increased slightly by 3 percent, and phishing websites with IP domains (for example, domains like http://255.255.255.255) increased significantly by about 147 percent. Webhosting services comprised 14 percent of all phishing, an increase of 1 percent from the previous month. The number of non-English phishing sites increased slightly by nearly 1 percent. Among the non-English phishing sites, sites in French and Italian continued to be higher in August.

The following trends are highlighted in the September 2010 report:

- Tale of .zip and .html Attachments
- A Phishing Scam Linked to “High School Musical”
- Phishers Target Automotive Sales Brands
- International Spam Roundup
- August 2010: Spam Subject Line Analysis
Metrics Digest

Global Spam Categories

<table>
<thead>
<tr>
<th>Category Name</th>
<th>August</th>
<th>July</th>
<th>Change (% points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>1%</td>
<td>1%</td>
<td>No change</td>
</tr>
<tr>
<td>Financial</td>
<td>9%</td>
<td>13%</td>
<td>-4</td>
</tr>
<tr>
<td>Fraud</td>
<td>4%</td>
<td>5%</td>
<td>-1</td>
</tr>
<tr>
<td>Health</td>
<td>12%</td>
<td>21%</td>
<td>-9</td>
</tr>
<tr>
<td>Internet</td>
<td>43%</td>
<td>33%</td>
<td>+10</td>
</tr>
<tr>
<td>Leisure</td>
<td>4%</td>
<td>3%</td>
<td>+1</td>
</tr>
<tr>
<td>419 spam</td>
<td>8%</td>
<td>7%</td>
<td>+1</td>
</tr>
<tr>
<td>Political</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>No change</td>
</tr>
<tr>
<td>Products</td>
<td>14%</td>
<td>13%</td>
<td>+1</td>
</tr>
<tr>
<td>scams</td>
<td>4%</td>
<td>3%</td>
<td>+1</td>
</tr>
</tbody>
</table>

Spam URL TLD Distribution

<table>
<thead>
<tr>
<th>TLD</th>
<th>August</th>
<th>July</th>
<th>Change (% points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td>67.0%</td>
<td>59.1%</td>
<td>+7.9</td>
</tr>
<tr>
<td>ru</td>
<td>13.0%</td>
<td>22.0%</td>
<td>-9.0</td>
</tr>
<tr>
<td>org</td>
<td>6.2%</td>
<td>6.1%</td>
<td>+0.1</td>
</tr>
<tr>
<td>info</td>
<td>4.8%</td>
<td>Not listed</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Average Spam Message Size

<table>
<thead>
<tr>
<th>Message Size</th>
<th>August</th>
<th>July</th>
<th>Change (% points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-2kb</td>
<td>12.02%</td>
<td>4.96%</td>
<td>+7.06</td>
</tr>
<tr>
<td>2kb-5kb</td>
<td>50.04%</td>
<td>59.97%</td>
<td>-9.93</td>
</tr>
<tr>
<td>5kb-10kb</td>
<td>27.42%</td>
<td>22.75%</td>
<td>+4.67</td>
</tr>
<tr>
<td>10kb+</td>
<td>10.52%</td>
<td>12.32%</td>
<td>-1.80</td>
</tr>
</tbody>
</table>

Spam Attack Vectors
Metrics Digest

Spam Regions of Origin

Geo-Location of Phishing Lures

Geo-Location of Phishing Hosts
Phishing Tactic Distribution

- Automated Toolkits: 16%
- Typosquatting: 2%
- Free Web Hosting Sites: 14%
- Other Unique Domains: 62%
- IP Address Domains: 6%

Phishing Target Sectors

- Financial: 87%
- Information Services: 12%
- Government: <1%
- Others: <1%
- Retail Trade: 54%
- ISPs: 41%
- Communications: 2%
- Retail: 2%
The chart displays the volume of spam messages containing attachments and messages containing .zip attachments since mid-June. Two major highlights are:

- Attachment spam as a whole increased significantly in August compared to the six weeks leading up to the month.
- The gap between the two lines of attachment spam and .zip attachment spam on the chart are much smaller in August, which indicates that .zip made up most of attachment spam.

Among the .zip attachment spam, there were three major categories:
- containing Trojan.Zbot variant
- containing Trojan.Sasfis variant
- Wavy pill messages

Trojan.Zbot has primarily been designed to steal confidential information from the computers it compromises. It specifically targets system information, online credentials, as well as banking details, and can be customized through the toolkit to gather any sort of information. It is primarily distributed through spam campaigns and drive-by downloads, which were not a surprise given the volume of messages Symantec has observed.

This email (right) claims to contain a legitimate attachment, using a variety of vectors to try to show its legitimacy. Some examples are also highlighted in Symantec blog posts available here and here. In this example, the spammer is using fake celebrity news to trick the user.
Tale of .zip and .html Attachments (continued)

Trojan.Sasfis is a Trojan horse that downloads and executes other malicious content. During August, spammers used a variety of shipping/delivery services brands to trick users.

The wavy images technique was highlighted in our July 2010 report. Rather than attaching the images, spammers started to zip the images and send the .zip attachment instead. This combined with two Trojans mentioned above made up vast majority of .zip attachment spam.

There was also an interesting development aside from the .zip attachment. In the first chart, the gap between the two lines widened towards the end of the month. This is attributed to an increase in .html attachment spam. These .html files contained malicious JavaScript, which can do the following:

- Exploit browser and plugin vulnerabilities to run arbitrary code
- Display fake antivirus scans and other fraudulent information
- Download JavaScript, HTML, and other files
- Hijack browsing sessions
- Redirect users to malicious websites
- Steal personal/confidential information

Symantec advises users to exercise caution when opening attachments in email messages. Users should also ensure that their operating system is up-to-date and a comprehensive security suite has been installed.
A Phishing Scam Linked to “High School Musical”

In August 2010, Symantec observed phishing websites spoofing a social networking brand that was linked to the film “High School Musical.” Typically, phishing sites are created to appear identical to the original website so that end users will find it difficult to distinguish between them. In the past couple of months, some phishing sites that spoofed social networking brands contained Web pages that were a bit different from the original.

So, why are fraudsters creating these phishing pages that aren’t identical to the original? These fraudsters are modifying the phishing site so that the page looks as though the brand was promoting certain ideas. In many instances, the ideas were associated with celebrities, special occasions, pornography, movies, major events, etc. These ideas are incorporated by modifying certain aspects of the phishing site such as the logo of the brand, Web page background, and images.

In this particular phishing site the fraudster included an image displayed as an advertisement for the social networking brand. The image was a picture of the popular film “High School Musical”. The phishing page gave the impression that the social networking brand was promoting the television film; this fake endorsement can be seen in the login message that prompted users to sign in to the brand’s High School Musical Web page:

The fraudsters’ motive was to trick customers into thinking that they could view the video or read and discuss more about the film after logging in to the site. Of course, once a user enters login details, the phishers succeeded in stealing the information for malicious purposes.

The phishing sites were hosted on free Web-hosting sites. The phishing URLs indicated that the content was linked to the High School Musical film. Below is an example of one such URL: http://*****/highschoolmusical.htm [Domain name removed]
Phishers Target Automotive Sales Brands

In the past couple of months, Symantec has observed phishing attacks on legitimate automotive sales brands that are based in the UK and the USA. These brands help customers to sell new and used vehicles such as cars and motorcycles. The legitimate websites also provide customers with the ability to advertise the vehicles they wish to sell.

There were several phishing sites created to harvest customers’ confidential information. The phishing sites were hosted on free Web hosting domains. In one of the phishing sites, the page stated that the brand was offering customers the opportunity to advertise for free. The customer was required to complete an identity verification (that was fake) to take advantage of the free offer. The verification process prompted for the customer’s email address, the ad’s ID, and a security question with an answer. In this attack the fraudsters attempted to convince customers that the phishing page was authentic by providing the caption “We fight fraud for you!!” On the contrary - if customers fall victim to the phishing site, the fraudsters will have succeeded in stealing their identities.

A second phishing site stated that the customer’s account was being kept “on-hold” and that he or she had to sign in to re-activate the account. After login information is entered, the page redirects to the legitimate site.

Still other phishing sites using similar scams asked for confidential information, including the customer’s contact details and credit card details. These particular phishing sites stated that the information was required to make a payment towards purchasing the vehicle that had been selected by the customer. The contact details requested included the customer’s name, address, phone number, and email address. The credit card details included the credit card number, card expiration date, and security code. The primary motive behind these phishing attacks was financial gain.
International Spam Roundup

There was an increase in spam volume which used Chinese Father’s Day as a promotion opportunity.

![Image of spam message promoting Chinese Father's Day]

In Russia, spammers have already started to prepare for the New Year. In this example, the spammer wants users to order 2011 calendars.

![Image of Russian spam message promoting calendars for 2011]

Last month’s report featured a Russian spam message promoting air-conditioners as the country suffered from heat waves. These heat waves also caused severe wildfires, and spammers were quick to take advantage of it in this message by promoting mask respirators. Another interesting characteristic is that this Russian message is written phonetically in English letters.
August 2010: Spam Subject Line Analysis

<table>
<thead>
<tr>
<th>#</th>
<th>Total Spam: August 2010 Top Subject Lines</th>
<th>No of Days</th>
<th>Total Spam: July 2010 Top Subject Lines</th>
<th>No of Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Your wife photos attached</td>
<td>21</td>
<td>Blank Subject line</td>
<td>31</td>
</tr>
<tr>
<td>2</td>
<td>Blank Subject line</td>
<td>31</td>
<td>Delivery Status Notification (Failure)</td>
<td>31</td>
</tr>
<tr>
<td>3</td>
<td>Your Order with Amazon.com</td>
<td>12</td>
<td>You have received an Greeting eCard</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>Meet Local Girls</td>
<td>16</td>
<td>Amazon.com: Please verify your new e-mail address</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>Resume</td>
<td>10</td>
<td>Returned mail: see transcript for details</td>
<td>31</td>
</tr>
<tr>
<td>6</td>
<td>Your private photo attached</td>
<td>7</td>
<td>Undelivered Mail Returned to Sender</td>
<td>31</td>
</tr>
<tr>
<td>7</td>
<td>New Message</td>
<td>17</td>
<td>Nikki Sent You A Message</td>
<td>15</td>
</tr>
<tr>
<td>8</td>
<td>Join my network on LinkedIn</td>
<td>4</td>
<td>My Pics</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>You have notifications pending</td>
<td>22</td>
<td>failure notice</td>
<td>31</td>
</tr>
<tr>
<td>10</td>
<td>Best Sales 2010!</td>
<td>3</td>
<td>Give your partner a one-way ticket to ecstasy-land.</td>
<td>31</td>
</tr>
</tbody>
</table>

As noted in the landscape summary, .zip attachment spam was the highlight of the month. This is reflected in the Subject Line Analysis as several of top ten rankings were .zip attachment spam messages.
Checklist: Protecting your business, your employees and your customers

Do
- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. De-select items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid publishing your email address on the Internet. Consider alternate options – for example, use a separate address when signing up for mailing lists, get multiple addresses for multiple purposes, or look into disposable address services.
- Using directions provided by your mail administrators report missed spam if you have an option to do so.
- Delete all spam.
- Avoid clicking on suspicious links in email or IM messages as these may be links to spoofed websites. We suggest typing web addresses directly into the browser rather than relying upon links within your messages.
- Always be sure that your operating system is up-to-date with the latest updates, and employ a comprehensive security suite. For details on Symantec’s offerings of protection visit http://www.symantec.com.
- Consider a reputable antispam solution to handle filtering across your entire organization such as Symantec Brightmail messaging security family of solutions.
- Keep up to date on recent spam trends by visiting the Symantec State of Spam site which is located here.

Do Not
- Open unknown email attachments. These attachments could infect your computer.
- Reply to spam. Typically the sender’s email address is forged, and replying may only result in more spam.
- Fill out forms in messages that ask for personal or financial information or passwords. A reputable company is unlikely to ask for your personal details via email. When in doubt, contact the company in question via an independent, trusted mechanism, such as a verified telephone number, or a known Internet address that you type into a new browser window (do not click or cut and paste from a link in the message).
- Buy products or services from spam messages.
- Open spam messages.
- Forward any virus warnings that you receive through email. These are often hoaxes.

* Spam data is based on messages passing through Symantec Probe Network.
* Phishing data is aggregated from a combination of sources including strategic partners, customers and security solutions.