



# THREATForecast

AND REPORT

The **monthly Spam Soap Threat Forecast & Report** provides IT leaders and messaging security professionals with information on recent and potential email and Web threats. The forecast relies on current and historical data and trends, as well as expert analysis of real time spam and virus events monitored and assessed by the 24x7 Threat Operations Center.

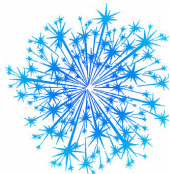
## July 2008 Threat Forecast

Despite last month's forecast that spam volume would increase, spam volume decreased for the fourth month in a row. However, spam volumes are still up 100% over this same time last year. Based on historical trends and the July 4th holiday in the US, Spam Soap forecasts spam levels to reverse this four-month trend and increase through the end of the month. In addition, the rise of the Srizbi botnet and summer storms in the US should also contribute to the rise in spam volume.



### IPHONE ATTACKS

Spam Soap expects significant spam, scams and malware campaigns surrounding the highly anticipated July 11th release of Apple's new iPhone. Scams will be especially prevalent if supply doesn't meet demand. There has already been an iPhone scam with malware component targeted towards Latin America:  
<http://securitylabs.websense.com/content/Alerts/3107.aspx>.



### JULY 4TH SUMMER STORM

Although it's hardly worth celebrating, the July 4th holiday marks the one-year anniversary of the Storm worm e-card campaign that several other Storm variants have since latch onto. Spam Soap expects to see Storm release another July 4th variant again this year.



### SRIZBI BOTNET REMAINS KING

The Srizbi botnet continues to account for about 50% of all spam volume circulating on Internet and does not appear to be slowing down. Spam Soap forecasts that as many as 2 of the top 15 worms circulating in July will be associated with either the Srizbi or Storm Botnets.



### WHEN IT RAINS, SPAM POURS

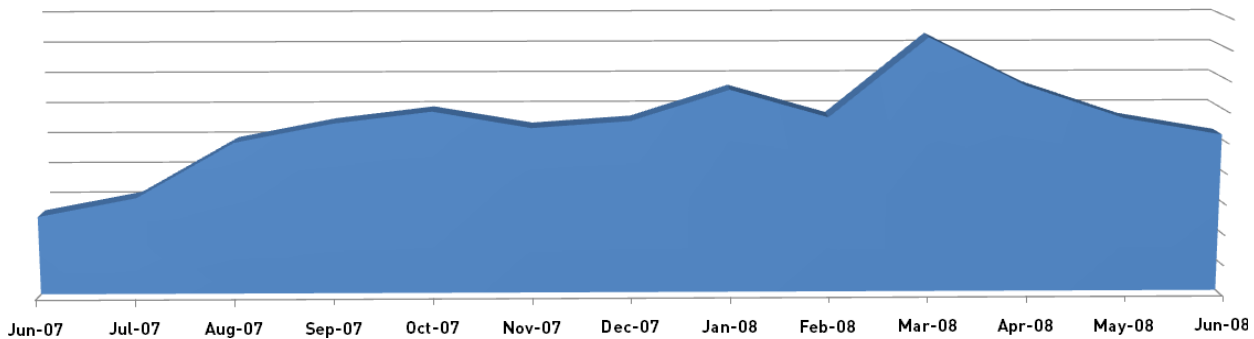
The warmer months generally bring more weather related issues such as the floods and tornadoes in the Midwest, wild fires out West and possible Hurricanes in the Gulf. Therefore, Spam Soap would expect to continue seeing heavy spam volumes related to these ongoing disasters.

## June 2008 Threat Report

### Spam Volume Down; Percentage Up

Despite last month's forecast of an increase, spam volume (the total number of spam messages) declined 10.5% from May to June. Spam volume is still up more than 100% over the same time last year. In addition, spam accounted for 89.1% of all email in June, up slightly from 87.6% in May.

#### SPAM VOLUME



#### Top 5 Categories

1. Health/Pharma (67.09%)
2. Offers (17.88%)
3. Image (2.20%)
4. Gambling (1.89%)
5. Foreign Language (1.17%)

#### Top 5 Viruses/ Worms

1. W32/Agent.TYW
2. Troj/Dorf-BN
3. W32/Agent.EHR
4. W32/Zhelatin.WT
5. W32/Srizbi-A

#### Top 5 Spam Countries

1. United States
2. Italy
3. Japan
4. Poland
5. United Kingdom

\*Malware in the "Agent" family are worms associated with distribution by the Srizbi botnet. Dorf is associated with Storm. So, Srizbi and Storm dominated our top 5 this month. Some of the "oldies but goodies" like Mytob and Nyxem were ranked 9th and 10th, respectively.

## Most Prevalent Types of Spam

### PORNTUBE SPAM

In late June, Spam Soap's Threat Operations Center tracked over 8 million messages related to the PornTube (accounting for over 85% of our worm traffic within a 24 hour period). This particular spam contained a link to a pornographic web site that contained an ActiveX malware component. It was determined that this malware appears to be related to the Srizbi botnet.

### ENHANCEMENT PRODUCT

Most of the health related spam has been one-liner spam with a link to a web site selling an enhancement product called PowerEnlarge.

In addition, several other smaller scams were recorded including some "Short and Distort" stock scams (opposite of Pump and Dump) in relation to the Amazon outage earlier this month, a new bogus message claiming that there was another earthquake in China, which was a variant of the Storm worm, and 419 phishing scams coming out of Google mail servers.

## The Best "Worst" Spam of the Month

In a common spam claiming to come from Microsoft announcing "10 lucky winners" of a Microsoft Lottery Program, the email attempts to lure recipients into providing detailed personal information in exchange for their prize. The message concludes with a warning:

"Warning!!! Any mail received of this such with any other trade mark or address should be forwarded to your claims processor immediately; this will help us to fight scam and lottery imposters. Thank you for your anticipated co-operation."

Talk about calling the kettle black.

