



THREAT Forecast AND REPORT

June 2009 Threat Forecast

The monthly Spam Soap® Threat Forecast and Report is designed to provide IT leaders and messaging security professionals with information on recent and potential email and Web threats. The forecast is developed using current and historical data and trends, as well as expert analysis of real time spam and virus events monitored and assessed by the 24x7 Spam Soap Threat Operations Center. To view the latest real-time data, visit www.spamsoap.com

WALEDAC SNEAK ATTACK?

It wouldn't be too surprising to see something new from the Waledac group in the next month or two. Their lack of recent activity in the malicious link spam email space lately leads us to think that the timing is ripe for them to return to the tactic, perhaps introducing a new, refreshed website intended to lure users into infecting their machines.

NEW SPIN ON OLD TACTIC

Over the last 8-9 months, a popular tactic has been to send fake invoices to potential customers of Western Union, UPS, DHL and FedEx claiming that their package could not be delivered. These customers are then instructed to print the attached, fake invoice, causing them to infect their computers. It's very likely that Cyber Criminals will attempt to increase their reach by sending generic messages to a much broader audience of recipients stating that they had a package or money transfer to pick up, instructing them to print the attached "claim form".

SPAM LEVELS PEAK

Over the last several months, we've observed spam levels rapidly return to pre-McColo shutdown levels, accounting for nearly 90 percent of all email in May. While we expect spam levels to climb slightly higher in June, it appears that all of the major spamming botnets are operating at full capacity.

JULY 4TH IS RIGHT AROUND THE CORNER

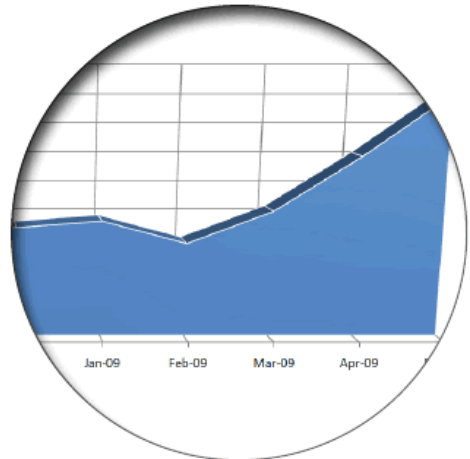
Although the ongoing global economic pressures will continue to inspire a large percentage of malicious messages throughout June, it's important not to lose sight of the upcoming July 4th holiday in the U.S. Expect July 4th-themed attacks toward the end of June.



May 2009 Threat Report

Spam volume continued its dramatic comeback, increasing nearly 35% in May. Since February 2009, spam volumes are up approximately 150%. Additionally, spam levels – the percentage of spam relative to legitimate email – also increased 1.1%, accounting for nearly 90% of all email traffic.

We haven't seen this spam volume since March 2008, when the industry saw a series of short-term bursts of spam. The current spam volumes, however, show no signs of letting up any time soon as all the major botnets – including Pushdo/Cutwail, Waledac, and Rustock – all appear to be operating at full strength.



(full chart on next page)

Total Spam Volume

+35%
From April



Spam Percentage

89.9%
Up from 88.8% in April



Top 5 Categories of Spam

1. Health
2. Offers
3. Foreign Language
4. Education
5. Phishing

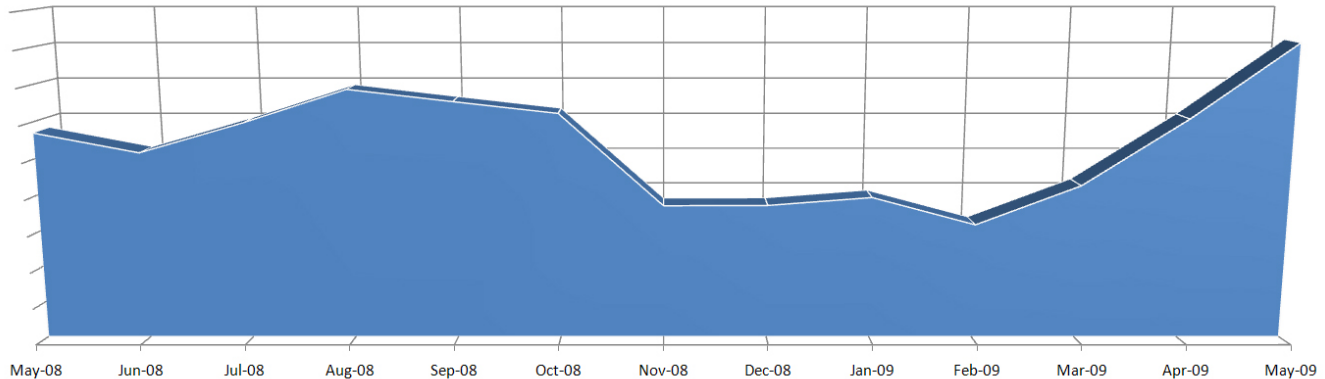
Top 5 Worms/Viruses

1. Troj/Agent-JUC
(Worldpay Scam)
2. Troj/Agent-JVF
(Western Union Scam)
3. Troj/Agent-JUZ
(Western Union Scam)
4. Troj/Agent-JZY
(Western Union Scam)
5. W32/Boza.C

Top 5 Spam Countries

1. United States
2. Brazil
3. Poland
4. Ukraine
5. Russian Federation

May 2009 Threat Report



Most Prevalent Spam and Malicious Messages of the Month

Health spam was once again the most prevalent type of spam during the month. What was notable this month, however, was the 10% increase that health spam represented relative to all spam. While an increase like this is notable, it essentially returns health spam back to the levels seen before the McColo shutdown late last year.

On a brighter note, we didn't observe a significant number of unique malicious spam campaigns during May. New malicious-link campaigns typically associated with the Waledac botnet were noticeably absent this month. Late in the month, emails purporting to be failed wire transfers made via Western Union did pick up in popularity. This Western Union tactic is very similar the UPS, DHL and FedEx scams we've seen since August 2008.

The Best "Worst" Spam of the Month

Processing more than a billion messages a day, we see our fair share of bogus emails, including funny ones, silly ones and downright scary ones too. Choosing just one Best "Worst" Spam of the Month is the hardest part.

So, we'd like to invite you to submit your favorites. Submit your favorite "Worst" spam by sending an email to support@spamssoap.com. Include a few sentences about the message and why you think it's worthy of mentioning.

If we select your spam message for next month's Best "Worst" Spam of the Month, we'll give you props in the next report as well as send you a free, semiused SecurityBuzz T-shirt.

HEADQUARTERS

Spam Soap, Inc.

3193 Red Hill Avenue
Costa Mesa, CA 92626

Phone: **1.866.SPAM.OUT** or 866.772.6688

Outside the U.S. call (001) 714.955.6959

Fax: 949.203.6425

Email: info@spamssoap.com

SALES

Email: sales@spamssoap.com

SUPPORT

Email: support@spamssoap.com