



# THREAT Forecast AND REPORT

## May 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](http://www.spamsoap.com)

### **FIRST MEGA-BOTNET COULD EMERGE**

Not long after the media mania surrounding Conficker died out in early April, Spam Soap researchers began noticing the infamous superbots began receiving periodic updates from a rival botnet gang, Waledac. This is highly unusual, and indicates that two of the world's largest botnets may be working together to create the first "mega-botnet" made up of tens or hundreds of millions of PCs.

### **THE SPAM HONEYMOON IS OFFICIALLY OVER**

Ever since the McColo shut down late last year, which reduced spam levels by nearly half, spammers have been making a slow comeback. That all changed in April, when we saw a nearly 40% spike in spam volume over the previous month. And there are no signs of it leveling off. In fact, we expect spam levels (percentage of spam to all email) to climb above 90% for the first time in more than seven months.

### **WASH YOUR HANDS AND EMAIL TOO**

Despite all the media attention surrounding the Swine Flu, we've seen relatively little spam about it to date. However, we anticipate that Swine Flu spam levels will increase as more spammers attempt to capitalize on people's ongoing curiosity and fear. So, add Swine Flu to the long list of social engineering tactics that spammers will try and use to sell people questionable products or infect their computers.

### **DON'T EXPECT SPAMMERS TO GROW A CONSCIENCE**

We'd love to tell you that we don't expect another flood of spam messages surrounding Mother's Day or Memorial Day, here in the US. Unfortunately, we can't. Both holidays are expected to generate a wave of malicious e-card or screen-saver downloads. These sort of malicious attacks have normally come from Waledac. However, given the recent cooperation between botnets, Conficker might become the new botnet of choice to propagate these threats.



# April 2009 Threat Report

## KABOOM!

Spammers put the pedal to the metal in April, increasing spam levels by 40% between March and April, and up more than 100% since February. Overall, spam accounted for 88% of all email sent, the highest levels seen since the shutdown of McColo last fall.

## CONFICKER MAKES FRIENDS

Conficker's April 1st "activation" day turned out to be anticlimactic. However, a few days later – and after all the media attention died off – Conficker-infected computers started downloading binary updates. While self-updating botnets are nothing new, what was unusual was this update was coming from a Waledac domain, another major botnet. This level of cooperation between two major botnets is interesting since rival botnets typically try to eradicate one another in an effort to establish supremacy.

### Total Spam Volume

**+40%**  
From March



### Spam Percentage

**88.8%**  
Up from 84.8% in March



### Top 5 Categories of Spam

1. Health
2. Offers
3. Non-English
4. Education
5. Phishing

### Top 5 Worms/Viruses

1. Troj/Agent-JNR
2. Troj/Agent-JNZ
3. Ma/EncPk-HZ
4. W32/Boza.C
5. Troj/Agent-JQF

### Top 5 Spam Countries

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

## Historical Spam Levels



## Most Prevalent Spam & Malicious Messages of the Month

Health and pill related spam typically pointing to pharmacy web sites, while seemingly always on the top of the list, managed to increase in volume as well as its percentage of overall spam last month. Last month health related emails comprised 59.9% of all spam, compared to 48.3, 45.0, 50.4, and 39.4% over the previous four month period.

Generic offer related spam has been on the decline for the past three months accounting for only 11.8% of spam email in April. Compare this to 16.0, 20.6, 19.8, and 25.2% over the past four months. The 25.2% observed in December (during the Christmas season) is about 8% over its historical two-year average indicating that retailers were primarily utilizing email as an inexpensive marketing vehicle to drive sales during an overall slow holiday season.

### ALL IS FAIR IN LOVE AND SPAM

The Waledac group's latest theme, a supposed short message service (SMS) spying utility, was April's most prevalent malicious spam campaign, attempting to capitalize on people's mistrust of their significant others. This theme appears have been a somewhat shorter run in comparison to their previous two campaigns, which included a fake coupon theme and a bomb scare video. Despite the campaign's brevity, there was no shortage of unique subject line topics, including:

- Are you ready to know the truth?
- Does your partner truly love you?
- Keep a spy eye on your girlfriend
- Do you trust her?
- Is your partner cheating on you?



## The Best “Worst” Spam of the Month

This month's best “Worst” spam was a no brainer. Simply read the section above about Waledac's SMS spying utility scam.

### 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@spamsoap.com](mailto:info@spamsoap.com)

### SALES

Email: [sales@spamsoap.com](mailto:sales@spamsoap.com)

### SUPPORT

Email: [support@spamsoap.com](mailto:support@spamsoap.com)