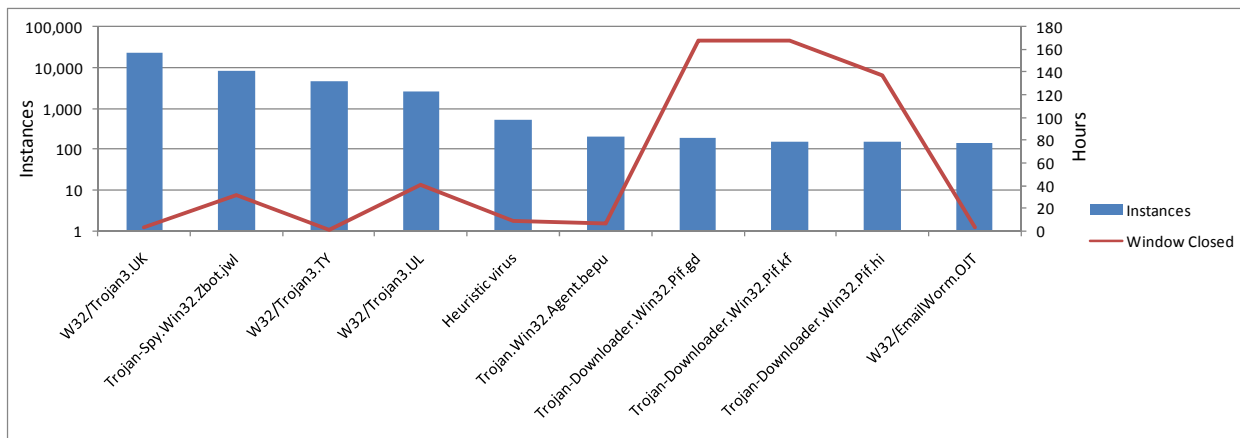


# In The Mail

## Monthly Websense Messaging Security Threat Brief



**Figure 1 – First to Detect**

This Month's Top 10 ThreatSeeker™ Malware Discoveries & the Window of Exposure closed by the ThreatSeeker™ Network. Because of ThreatSeeker, our Messaging Security customers are protected hours, or often days, before other security vendors provide a solution.

## KEY STATS

Threats "in the mail" this month:

- 3.0 billion messages were processed by the Hosted Infrastructure or over an average of 96.7 million messages/day
- 87.9% of all email was spam
- 91.7% of spam included an embedded URL
- 1.2 million instances of 535 unique zero-day threats stopped by ThreatSeeker before AV over the last 90 days
- 2.9% of all spam messages were phishing spam

How Websense is addressing these threats:

- Spam detection rate 99.8%. Websense Hosted Email Security provides 99% spam detection Service Level Agreement.
- Average false positive rate of 1 in 466,173
- 4.2% average daily threats protected using ThreatSeeker intelligence before AV signatures were available

What this means:

- The threat landscape is dangerous and growing more sophisticated.
- Websense is on the forefront of finding these threats including the increasingly pervasive blended threats.
- Most importantly, Websense is ideally positioned to address these threats with our market-leading Web security expertise, which drives our leadership in protecting from converged email & Web 2.0 threats.

## Cashing in on a Crisis

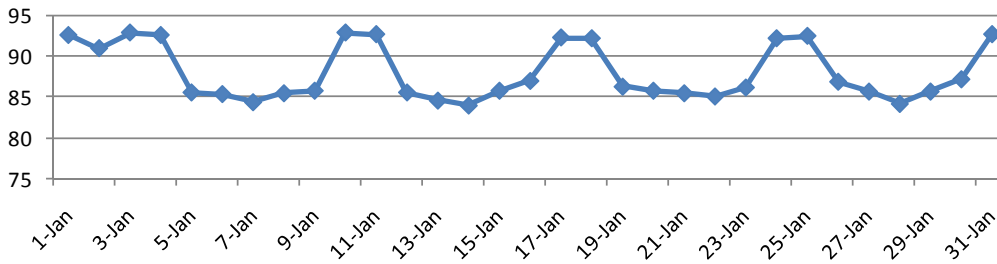
*Monthly Email Trends from the Security Labs*

Spammers use of the ongoing global financial crisis to lure users in to phishing scams was evident in [HMRC](#), [IRS 'Stimulus Payment'](#), and [Canada Revenue Agency #CRA tax refund](#) phishing attacks.

Spammers continue [relying on trusted reputation](#) of big Internet players to promote their [products and services](#). In an effort to reach their prospective customers spammers have increased their attack sophistication, which was clearly evident in some recent attacks.

Visual social engineering tactics has always been common and abundantly used practice by spammers, phishers and malware authors to increase chances of success with their email and web-based attacks. This was evident with some of recent phishing attacks corresponding to [CNN emails themed with Israel-Gaza conflict](#) and [Northwest Airlines Fake emails](#).

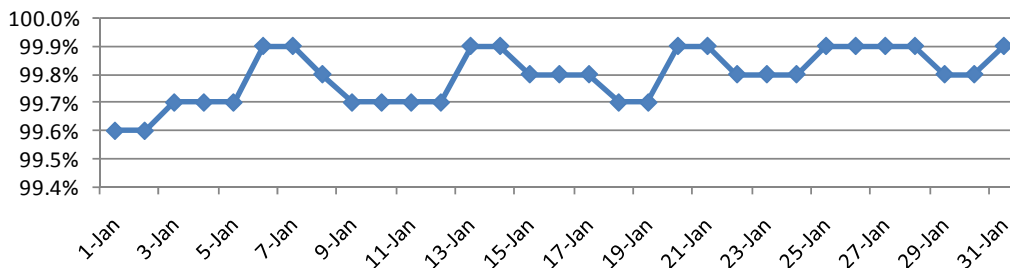
## Spam as a Percent of Inbound Email



**Figure 2 - Percent of email that contains spam (Average 87.9%)**

While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong messaging security solution, customers will experience bandwidth and storage capacity issues, frustration, and a drain in productivity, not to mention exposure to significant security risk.

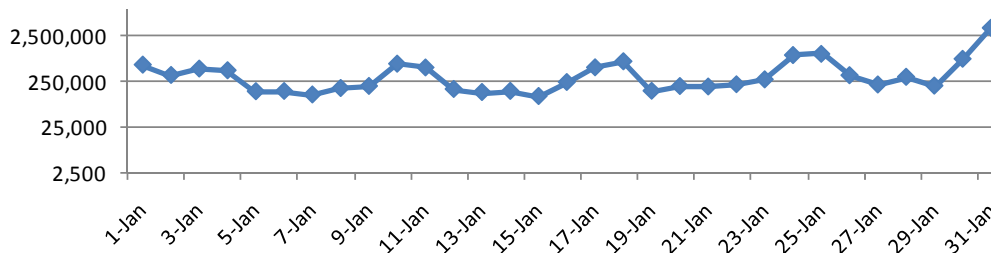
## Spam Detection Rate



**Figure 3 - Percent of spam detected (Average 99.8%)**

This is evidence that we are consistently maintaining a very high spam detection rate. Therefore, customers should be very confident that with Websense they are receiving the best in anti-spam protection.

## False Positive Rate (1 in X)



**Figure 4 - False Positive Rate (Average 1 in 466,173)**

This shows how Websense is consistently maintaining a very low false positive rate. While Websense is catching a high percentage of spam, customers are rarely inhibited by messages falsely landing in a spam queue.

## Why Websense Messaging Security?

- The Websense ThreatSeeker Network provides the intelligence to proactively protect against spam and malware – far ahead of traditional anti-spam and anti-virus alone.
- Today's pervasive blended threats are best matched by integration of best-in-class Websense Web security with email security for Essential Information Protection.