

In The Mail

Monthly Websense Email Security Threat Brief

Top 10 Classifications of URLs in Email

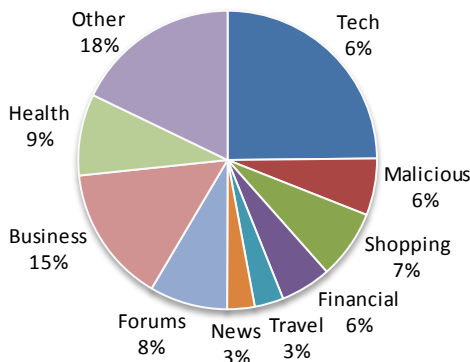


Figure 1: Embedded URLs in Email
Understanding how Web URLs in Email are classified is crucial to stopping converged threats

Top 10 ThreatSeeker™ Malware Discoveries & Closed Window of Exposure

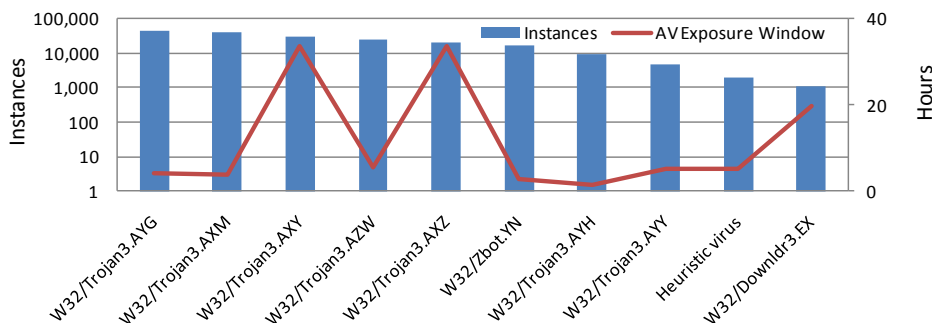


Figure 2: First to Detect
Because of the ThreatSeeker™ Network, our Email Security customers are protected hours, and often days, before other security vendors provide a solution.

KEY STATS

Threats “in the mail” this month:

- 3.2 billion messages processed by the Hosted Infrastructure (over 107 million per day)
- 87.5% of all email was spam
- 84.9% of spam included an embedded URL
- 217 thousand instances of 49 unique zero-day threats stopped by ThreatSeeker before AV
- 2.1% of spam emails were phishing attacks

How Websense is addressing these threats:

- 99.7% spam detection rate. Websense Hosted Email Security provides 99% spam detection Service Level Agreement.
- Average false positive rate of 1 in 216,587
- 11.6% 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.

Tragedy Exploited

Monthly Email Trends from the Security Labs

Within 24 hours of Michael Jackson's sudden death, spammers sent out malicious emails using a [fake video](#) of the singer's death as a social engineering lure. The Websense ThreatSeeker Network detected these emails and the compromised Web site that they linked to that contained information stealing malware. We saw continued use of the singer's name as a lure to promote everything from pharmacy websites to other malicious downloads hosted on purposely created Web sites.

The total number of emails detected as containing viruses increased six-fold in June. Also, we saw an increase in the number of phishing emails using attached HTML forms. ThreatSeeker uses knowledge of the many attributes of emails to successfully determine their malicious nature. This provides accurate detection of attacks such as shipping company notifications which have started to mix in embedded URLs along with attachments, as well as low volume highly-targeted attacks.

Spam as a Percent of Inbound Email

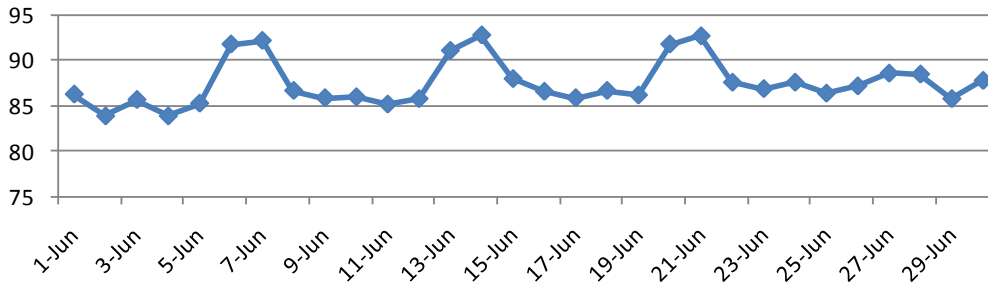


Figure 3 - Percent of email that contains spam (Average 87.5%)

While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong email 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

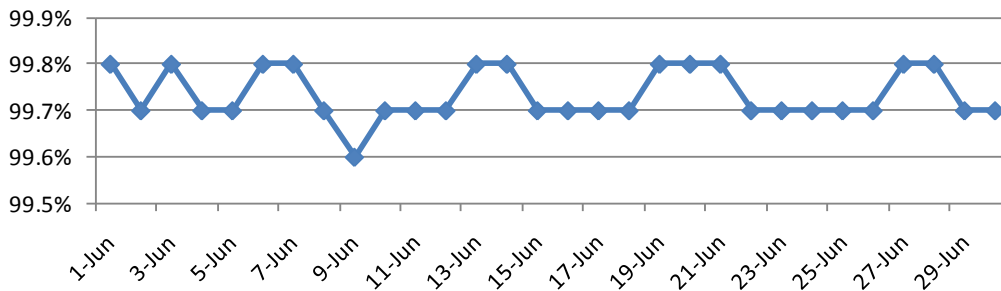


Figure 4 - Percent of spam detected (Average 99.7%)

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)

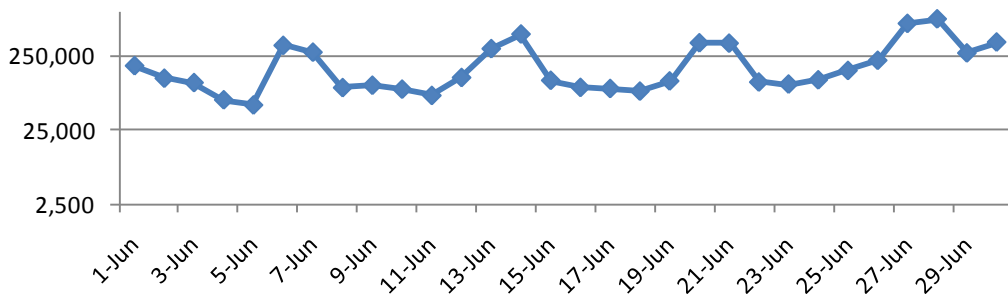


Figure 5 - False Positive Rate (Average 1 in 216,587)

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 Email 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.