

# In The Mail

## Monthly Websense Email Security Threat Brief

Top 10 Classifications of URLs in Email

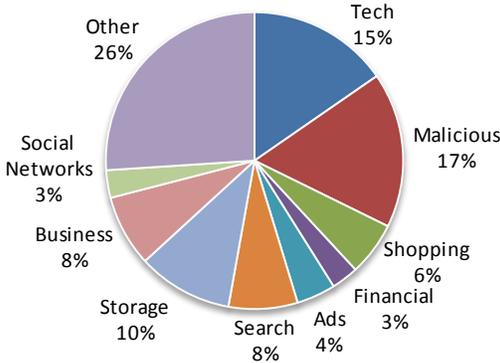


Figure 1: Embedded URLs in Email

Understanding how Web URLs in Email are classified is crucial to stopping converged threats

Top 10 ThreatSeeker™ Malware Discoveries & Closed Window of Exposure

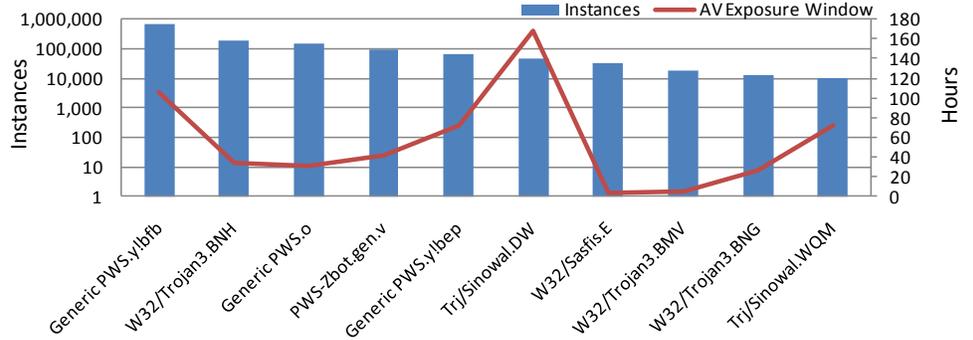


Figure 2: First to Detect

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:

- 3.0 billion messages processed by the Hosted Infrastructure (over 98 million per day)
- 84.1% of all email was spam
- 86.1% of spam included an embedded URL
- 1.5 million instances of 63 unique zero-day threats stopped by ThreatSeeker before AV
- 2.1% of spam emails were phishing attacks

How Websense is addressing these threats:

- 99.8% spam detection rate. Websense Hosted Email Security provides 99% spam detection Service Level Agreement.
- Average false positive rate of 1 in 257,985
- 12.5% 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.

## Holiday Spam Scams

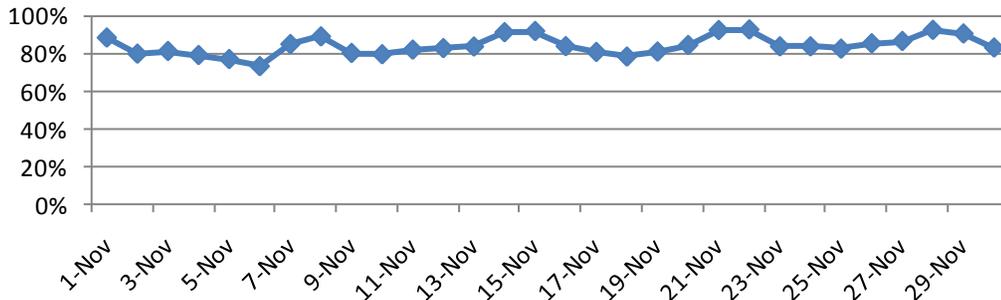
Monthly Email Trends from the Security Labs

Just like any business owner, spammers have been using holidays to increase their revenue. October brought Halloween themed spam, and in early November spammers capitalized on the [U.S. Veteran's Day holiday](#). They're using discounts, free shipping, combo packs, and free samples with purchase, among other marketing strategies, to lure their victims. We can expect even more in the days to come.

A [Visa phishing](#) campaign targets holiday shoppers who buy gifts online. The attack attempts to exploit the "[Verified By Visa](#)" program. The phishing email redirects the victim to a spoofed page that harvests all the information the victim provided the card-issuing bank at the time of sign up for the credit card.

A facebook phishing attempt was [reported](#) that aims to harvest facebook credentials. Once the victim enters a username and the password, he or she is redirected to an error message claiming an "incorrect email/password combination".

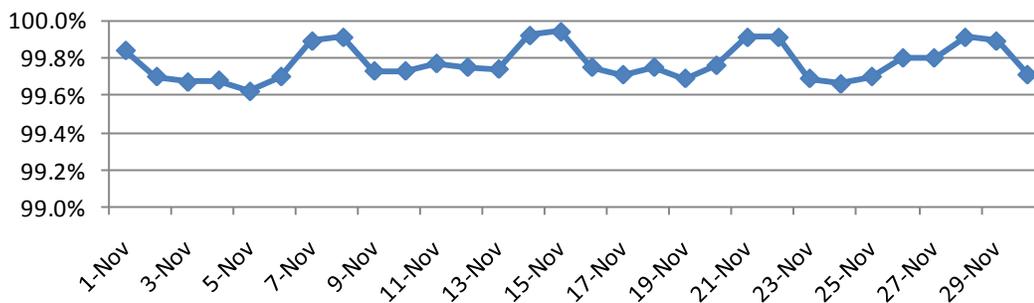
## Spam as a Percent of Inbound Email



**Figure 3 - Percent of email that contains spam (Average 84.1%)**

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.

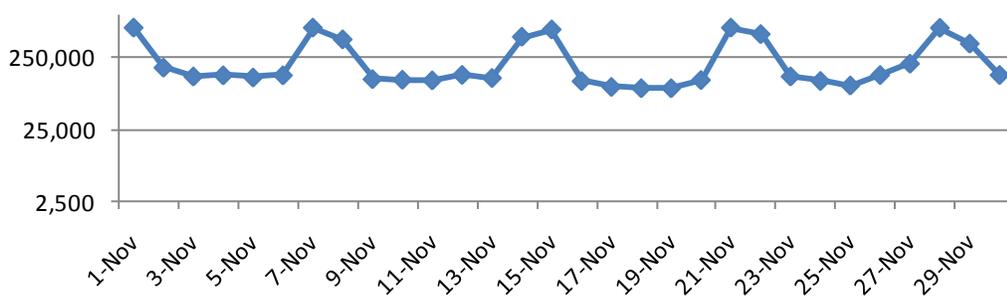
## Spam Detection Rate



**Figure 4 - Percent of spam detected (Average 99.8%)**

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 5 - False Positive Rate (Average 1 in 257,985)**

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.