

In The Mail

Monthly Websense® Messaging Security Threat Brief with Statistics from the Websense Security Labs

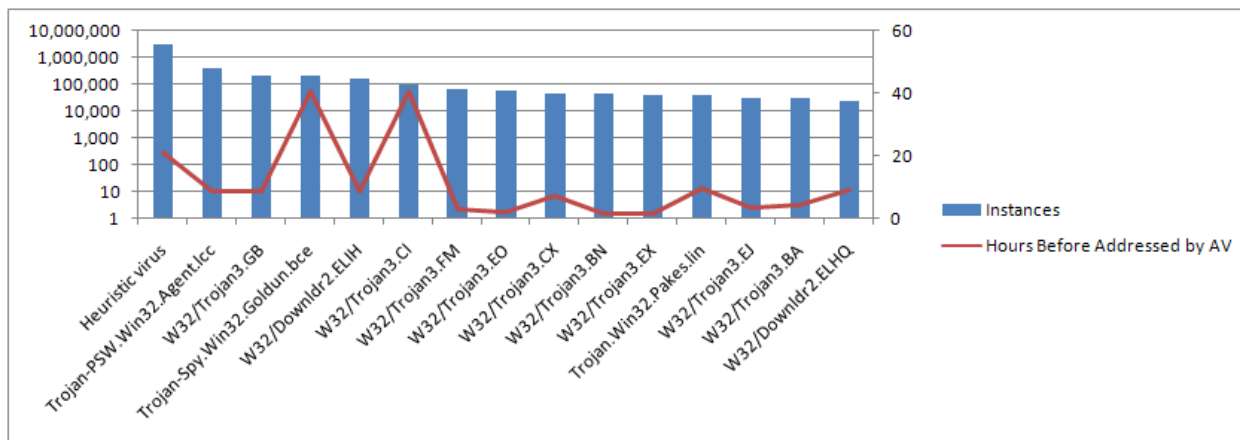


Figure 1 – First to Detect

This Month's Top 15 Websense ThreatSeeker™ Network Malware Discoveries & the Window of Exposure before AV solutions addressed the threat (in instances and hours). Because of the Websense ThreatSeeker Network, our Messaging Security customers are protected hours, or often days, before other security solutions can provide a solution.

KEY STATS FROM THE WEBSENSE SECURITY LABS

Threats "in the mail" this month:

- 3.2 Billion messages were processed by the Hosted Infrastructure or over an average of 103 Million messages/day
- 82.9% of all email was spam
- 90.5% of spam included an embedded URL
- 5 Million instances of 413 unique zero-day viruses found before AV
- Longest window of exposure to zero-day viruses before an AV signature was made available: 1 week
- 3 in 50 messages were phishing sites (An increase of 240%+ over last month!)

How Websense is addressing these threats:

- Spam detection rate 99.75% (IronPort advertises greater than 98%*)
- Average false positive rate of 1 in 284,938 (Barracuda claims a rate of approximately 1 in 100**)
- 18.1% of threats protected using Websense ThreatSeeker Network 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.

Gone Phishing

Monthly Email Trends from the Websense Security Labs

[Rock Phishers](#) with their fast-flux [infrastructure](#) have once again indicated their interest in obtaining the user account credentials, using [mass](#) phishing campaigns targeting banks (recent attacks reported on Suntrust, Lloyds, and Bank of America). SANS Internet Security Center [reports](#) that a well-formatted phish can score about a 10% click-through rate, whereas a targeted phish can score upwards of 80%.

The phishing authors continue to push several [sophisticated crimeware packages](#) that get silently installed on the victim's PC.

Another emerging trend in phishing are [phishes that bite back](#) - when the Web site form is filled with junk information.

Spam as a Percent of Inbound Email

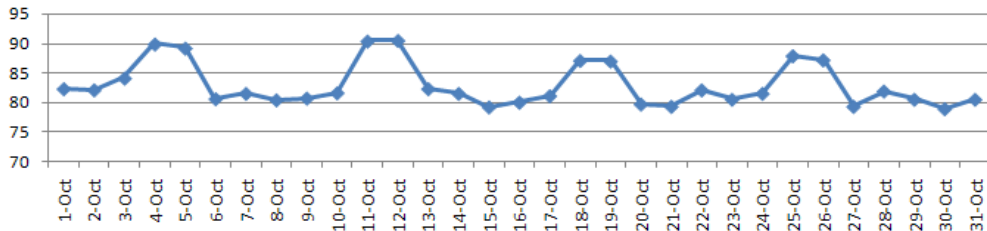


Figure 2 - Percent of Email Detected as SPAM over last month (Average 82.9%)
 While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong Messaging Security solution, customers will experience bandwidth and storage capacity issues, frustration, and a drain in productivity, not to mention exposure to significant security risk.

Spam Detection Rate

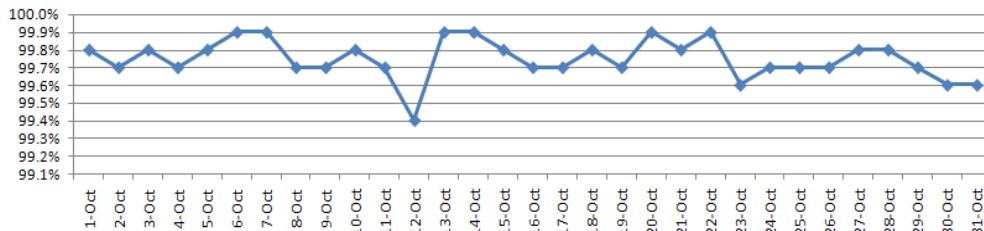


Figure 3 - Percent of Email Detected as Spam (Average 99.75%)
 This is evidence that we are consistently maintaining a very high Spam detection rate. Therefore, customers should be very confident that with Websense they are receiving the best in anti-spam protection.

False Positive Rate (1 in X)

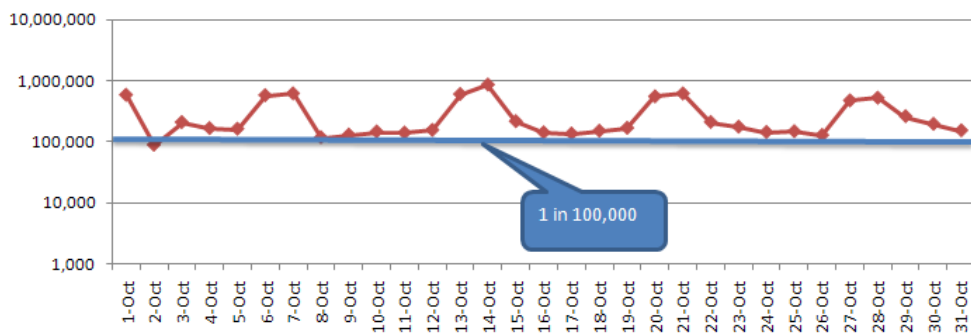


Figure 4 - False Positive Rate (Average 1 in 284,938)
 This shows how Websense is consistently maintaining a very low false positive rate. While Websense is catching a high percentage of spam, customers are rarely inhibited by messages falsely landing in a spam queue.

Why Websense Messaging Security?

- The Websense Threat Seeker 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.

*Source: www.ironport.com
 **Source: www.barracuda.com