

In The Mail

Monthly Websense Email Security Threat Brief

Top 10 Classifications of URLs in Email

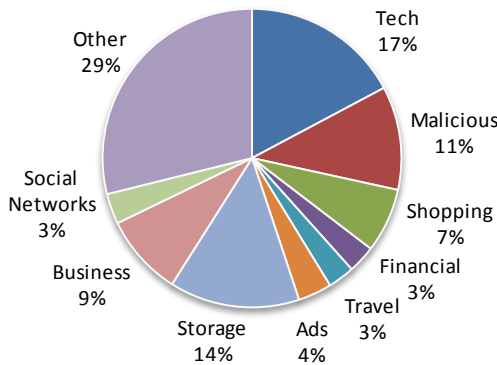


Figure 1: Embedded URLs in Email
Understanding how Web URLs in Email are classified is crucial to stopping converged threats

Top 10 ThreatSeeker™ Malware Discoveries & Closed Window of Exposure

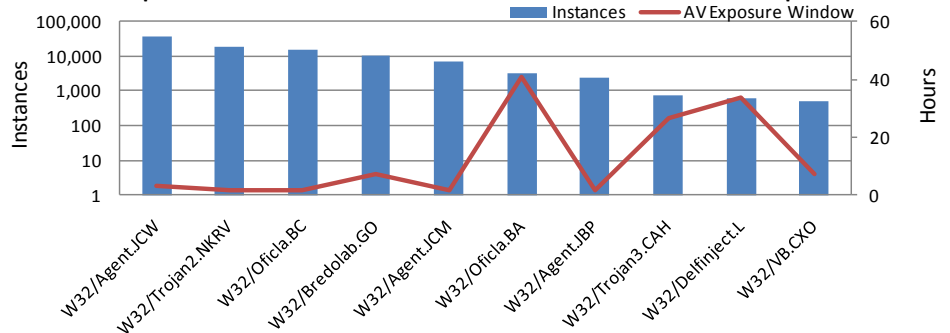


Figure 2: First to Detect
Because of the ThreatSeeker™ Network, our Email Security customers are protected hours, and often days, before other security vendors provide a solution.

KEY STATS

Threats "in the mail" this month:

- 4.7 billion messages processed by the Hosted Infrastructure (over 158 million per day)
- 82.1% of all email was spam
- 84.9% of spam included an embedded URL
- 186 thousand instances of 81 unique zero-day threats stopped by ThreatSeeker before AV
- 0.7% 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 753,624
- 10.4% 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.

Here You Have

Monthly Email Trends from the Security Labs

This month we saw an old trick involving a .scr file masquerading as a .pdf file using the "[Here You Have](#)" malicious emails. Why reinvent the wheel when you can recycle methods and processes, in this case the use of an old worm being spread using different means. Surprisingly, this escaped most AV engines as verified on [VirusTotal](#).

Jumping on the band wagon of using any means to get users' attention and to propagate attacks, this month saw further blended attacks employing everyday tools we have grown accustomed to such as [Skype](#)-themed malicious emails and [Facebook](#) password reset emails leading users to rogue AV downloads.

The intriguing aspect of these blended attacks is what happens in the background, unknown to the user. One might think they have only been redirected to a rogue AV site, but they may have kicked off a chain reaction with redirects to an exploit site where an exploit kit or other damaging content is downloaded to the user's machine.

This month demonstrates two things: 1) Spammers will use any means to propagate their malware and 2) Special attention needs to be paid to blended attacks.

Spam as a Percent of Inbound Email

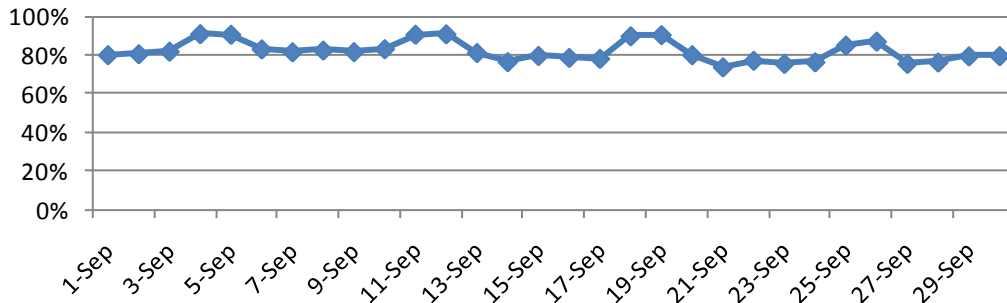


Figure 3 - Percent of email that contains spam (Average 82.1%)

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 (Ave 99.7%)

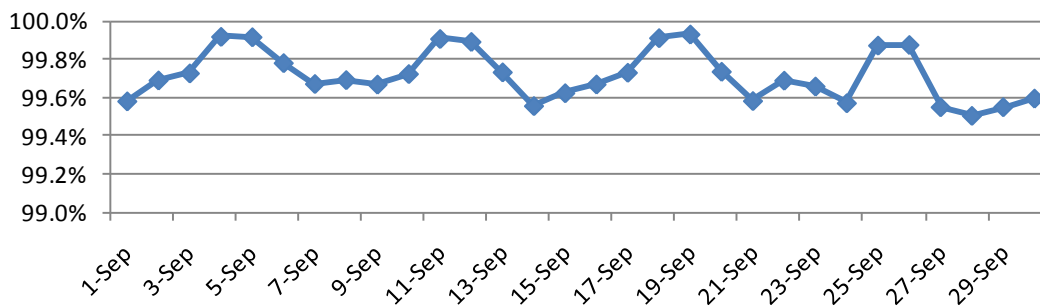


Figure 4 - Percent of spam detected

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

False Positive Rate (1 in 753,624)

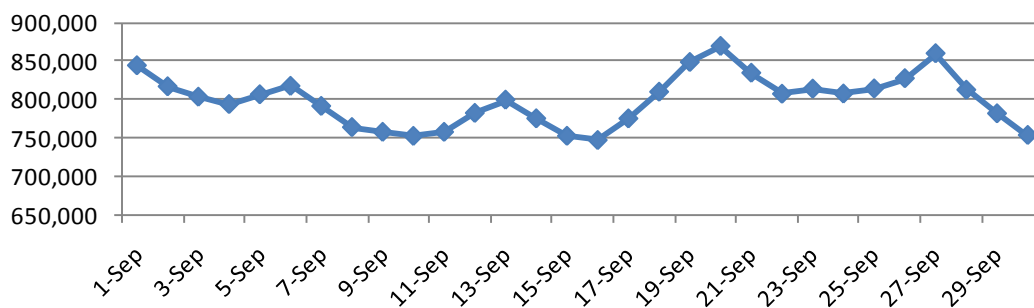


Figure 5 - False Positive Rate (30 Day Rolling Average)

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.