
## Monthly Websense Email Security Threat Brief

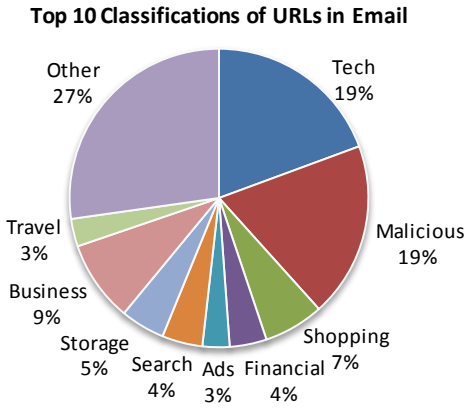


**Figure 1: Embedded URLs in Email**
Understanding how Web URLs in Email are classified is crucial to stopping converged threats

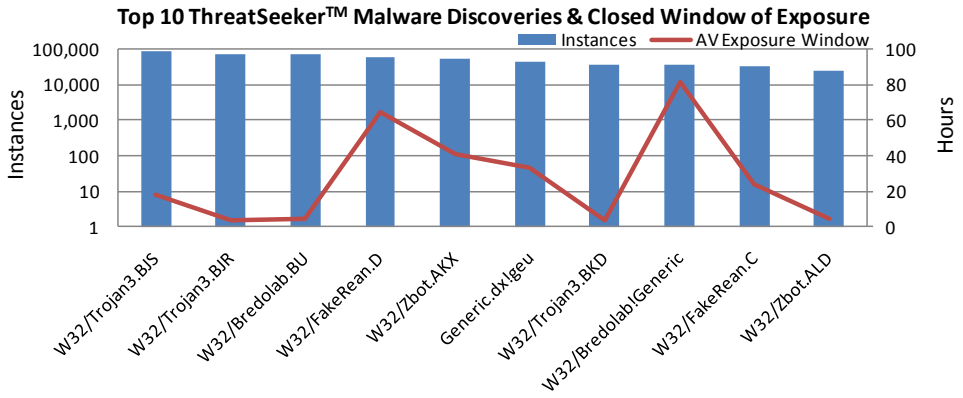


**Figure 2: First to Detect**
Because of the ThreatSeeker™ Network, our Email Security customers are protected hours, and often days, before other security vendors provide a solution.

### KEY STATS

Threats "in the mail" this month:

- 3.0 billion messages processed by the Hosted Infrastructure (over 98 million per day)
- 81.7% of all email was spam
- 83.3% of spam included an embedded URL
- 870 thousand instances of 90 unique zero-day threats stopped by ThreatSeeker before AV
- 1.7% of spam emails were phishing attacks

How Websense is addressing these threats:

- 99.6% spam detection rate. Websense Hosted Email Security provides 99% spam detection Service Level Agreement.
- Average false positive rate of 1 in 837,490
- 19.3% 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.

# Cyber Crooks Cash In

*Monthly Email Trends from the Security Labs*

The FBI announced that cyber crooks have stolen $40M from small and mid-sized firms in the U.S. The perpetrators stole online banking credentials by using malicious software distributed via spam. This information was then used to make a series of unauthorized bank transfers from the victims to money mules, who then wired the money to the bad guys after taking a commission.

There was a slew of phishing attacks on U.K. nationals purporting to be from the HMRC (the U.K.'s tax collection agency) offering tax rebates—but first asking the victim to enter their bank account or credit card details. A total of 83,000 emails were discovered, with 10,000 of them arriving in just one day.

Around 10,000 Hotmail passwords were posted online by an anonymous user. These passwords were likely obtained via a phishing scheme. An analysis of the passwords has been posted on Acunetix: 69% of the passwords were between 6 and 9 characters long, the most common password was "123456", and all the top 20 passwords that did not involve numbers were dictionary words.

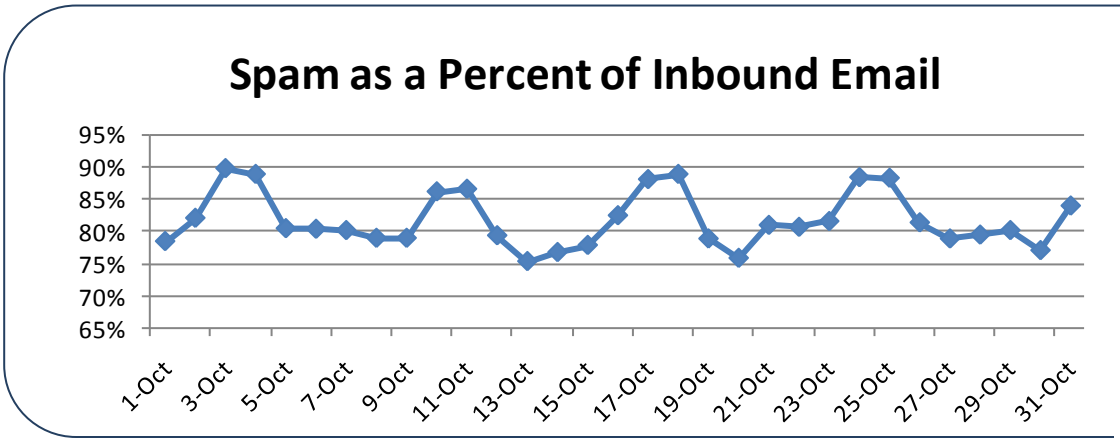


**Figure 3 - Percent of email that contains spam (Average 81.7%)**
While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong email security solution, customers will experience bandwidth and storage capacity issues, frustration, and a drain in productivity, not to mention exposure to significant security risk.

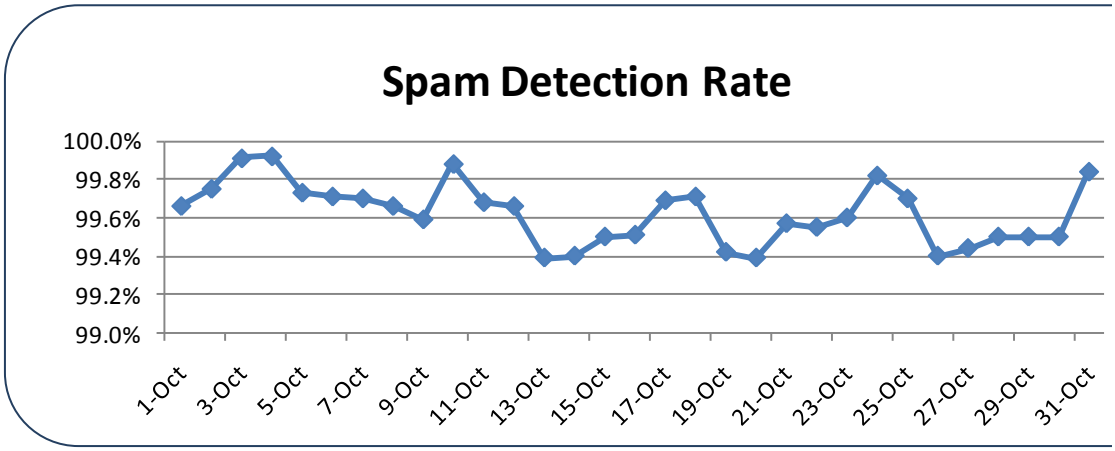


**Figure 4 - Percent of spam detected (Average 99.6%)**
This is evidence that we are consistently maintaining a very high spam detection rate. Therefore, customers should be very confident that with Websense they are receiving the best in anti-spam protection.

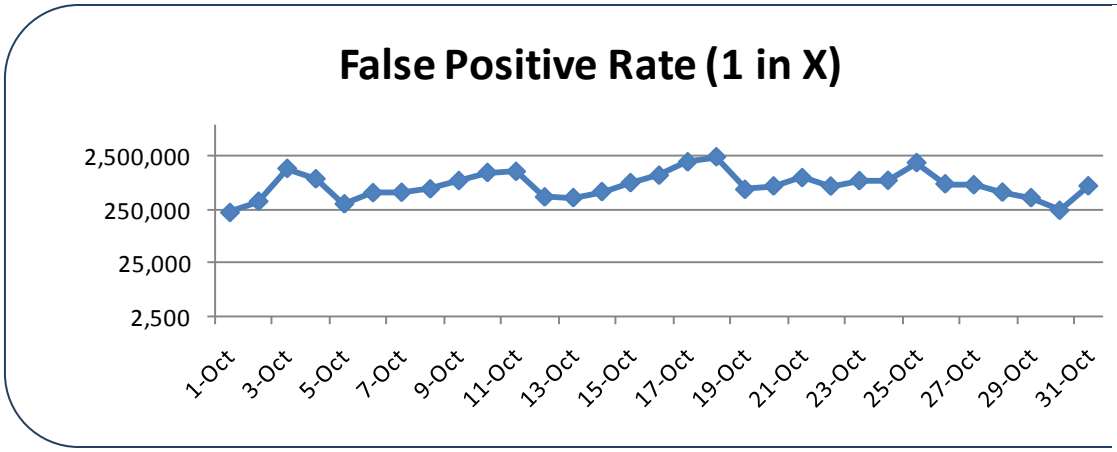


**Figure 5 - False Positive Rate (Average 1 in 837,490)**
This shows how Websense is consistently maintaining a very low false positive rate.
While Websense is catching a high percentage of spam, customers are rarely inhibited by messages falsely landing in a spam queue.

**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.