Monthly Websense Email Security Threat Brief

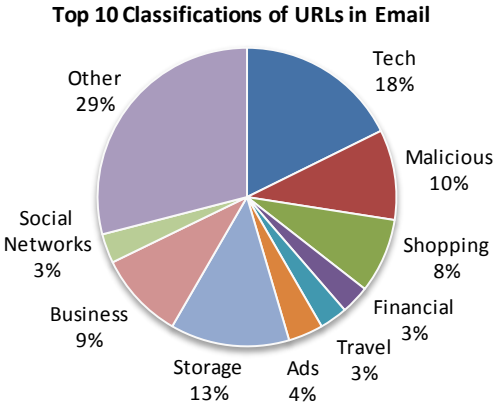

Figure 1: Embedded URLs in Email
Understanding how Web URLs in Email are classified is crucial to stopping converged threats

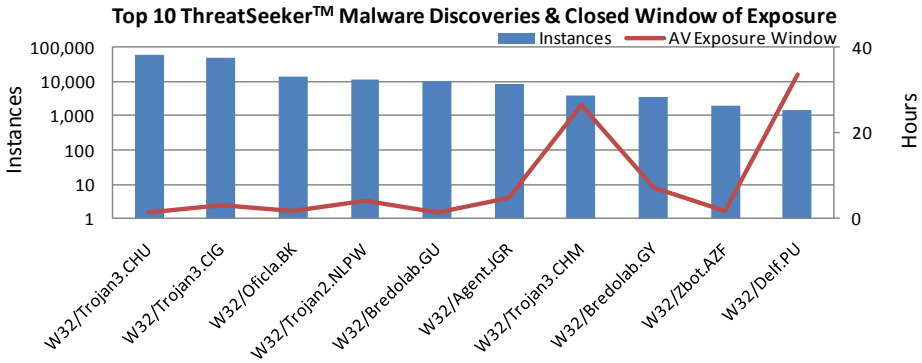

Figure 2: First to Detect
Because of the ThreatSeeker™ Network, our Email Security customers are protected hours, and often days, before other security vendors provide a solution.

KEY STATS

Threats "in the mail" this month:

- 4.5 billion messages processed by the Hosted Infrastructure (over 149 million per day)
- 80.7% of all email was spam
- 82.2% of spam included an embedded URL
- 295 thousand instances of 86 unique zero-day threats stopped by ThreatSeeker before AV
- 0.8% 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 632,098
- 15.2% 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.

The Big Phish

Monthly Email Trends from the Security Labs

An increase in the number of phishing emails has been a focal point over the course of this month. Most of them seem to be directed attacks at Email Service Providers (ESPs) in order for the attackers to gain access to "industry-grade email deployment systems". Spear-phishing, as it is known to most, is on the rise with several of these messages having the look and feel of legitimate requests to the unsuspecting user. Like most of the email campaigns reported in the past, the format is usually the same: A user is lured into clicking a link within an email or to open an attachment, which results in the machine being infected.

Also this month, with the release of the new version of Adobe Reader, came the recycled phishing email messages enticing and advising users to upgrade their readers to the improved version with all the bells and whistles. As reported in Lenny Zeltser's blog, the format of these messages did not change much. These types of email messages are not new, although it is interesting to note that cyber-criminals are keeping abreast of current changes and news and taking advantage of them.

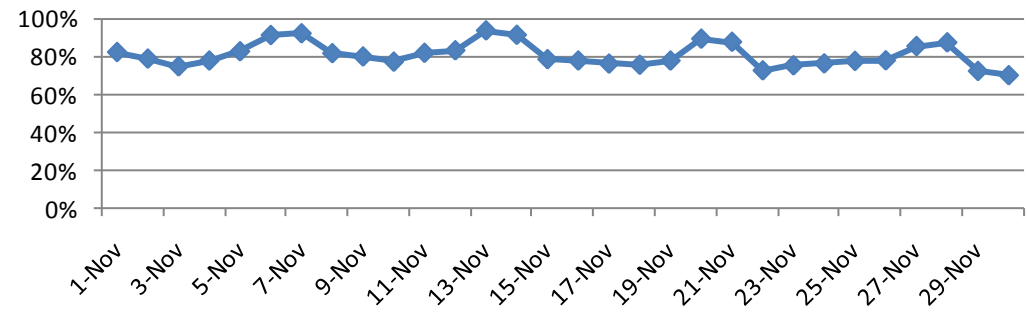

Figure 3 - Percent of email that contains spam (Average 80.7%)
While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong email security solution, customers will experience bandwidth and storage capacity issues, frustration, and a drain in productivity, not to mention exposure to significant security risk.

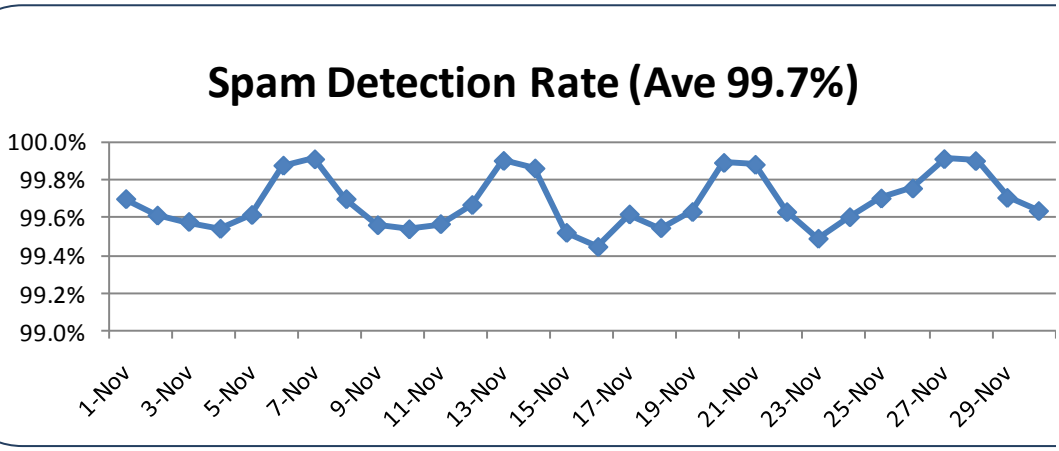

Figure 4 - Percent of spam detected
This is evidence that we are consistently maintaining a very high spam detection rate. Customers should be very confident that with Websense they are receiving the best in anti-spam protection.

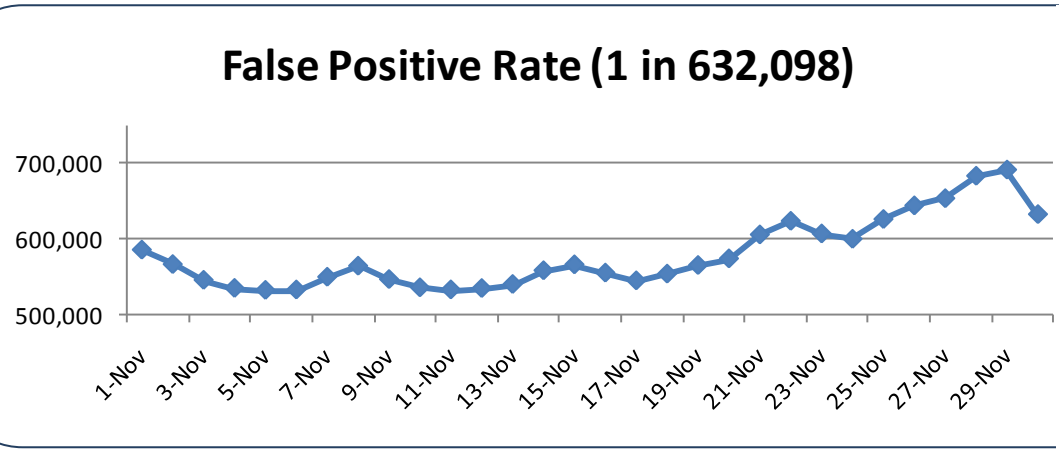

Figure 5 - False Positive Rate (30 Day Rolling Average)
This shows how Websense is consistently maintaining a very low false positive rate.
While Websense is catching a high percentage of spam, customers are rarely inhibited by messages falsely landing in a spam queue.

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.