Monthly Websense Email Security Threat Brief

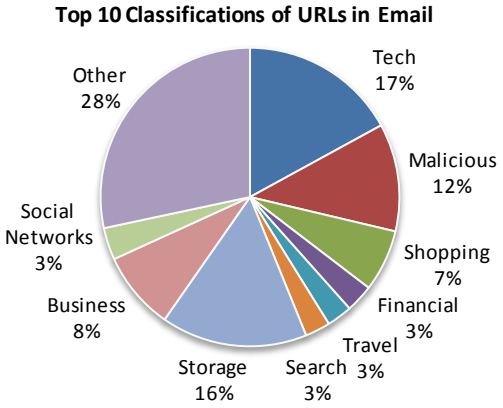

Figure 1: Embedded URLs in Email
Understanding how Web URLs in Email are classified is crucial to stopping converged threats

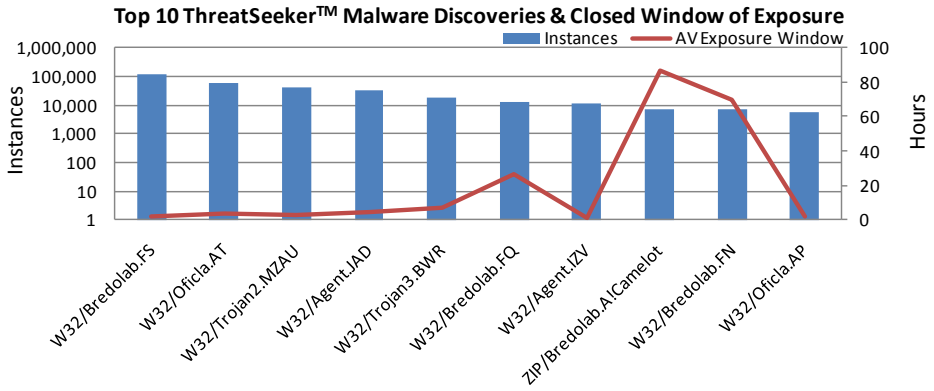

Figure 2: First to Detect
Because of the ThreatSeeker™ Network, our Email Security customers are protected hours, and often days, before other security vendors provide a solution.

KEY STATS

Threats "in the mail" this month:

- 4.6 billion messages processed by the Hosted Infrastructure (over 148 million per day)
- 84.5% of all email was spam
- 81.9% of spam included an embedded URL
- 479 thousand instances of 99 unique zero-day threats stopped by ThreatSeeker before AV
- 0.8% 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 1,041,020
- 23.5% 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.

Brand Jacking

Monthly Email Trends from the Security Labs

Websense Security Labs™ ThreatSeeker™ Network has detected thousands of malicious emails purporting to be from big-brand companies like Target, Macy's, Best Buy, and Evite. These malicious emails all leverage the fake AV strategy that we blogged about two months ago. The malicious URLs in the emails redirect to the same fake AV web site where users are then prompted to run a malicious executable called "antivirus_24.exe", currently only detected by 11 out of 42 AV engines.

While "brand-jacking" certainly isn't new, this month Gumblar seems to have made a comeback impersonating Amazon.com. The aim of the campaign was to trick unsuspecting users to visit a client-side exploit serving URL.

Other attacks include but are not limited to the influx of Youtube themed spam requesting users to confirm their email address, the fake ImageShack Registration emails, and Welcome to My Opera account. In addition, there was no shortage or end to the abuse of social networking sites such as Facebook and hi5.

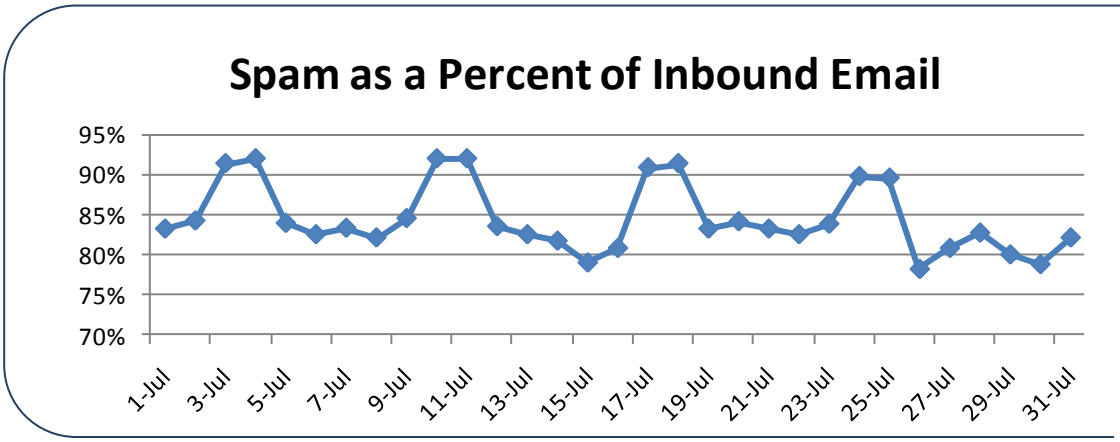

Figure 3 - Percent of email that contains spam (Average 83.7%)
While this figure fluctuates, this signifies that a very high percentage of incoming email is indeed spam. Without a strong email security solution, customers will experience bandwidth and storage capacity issues, frustration, and a drain in productivity, not to mention exposure to significant security risk.

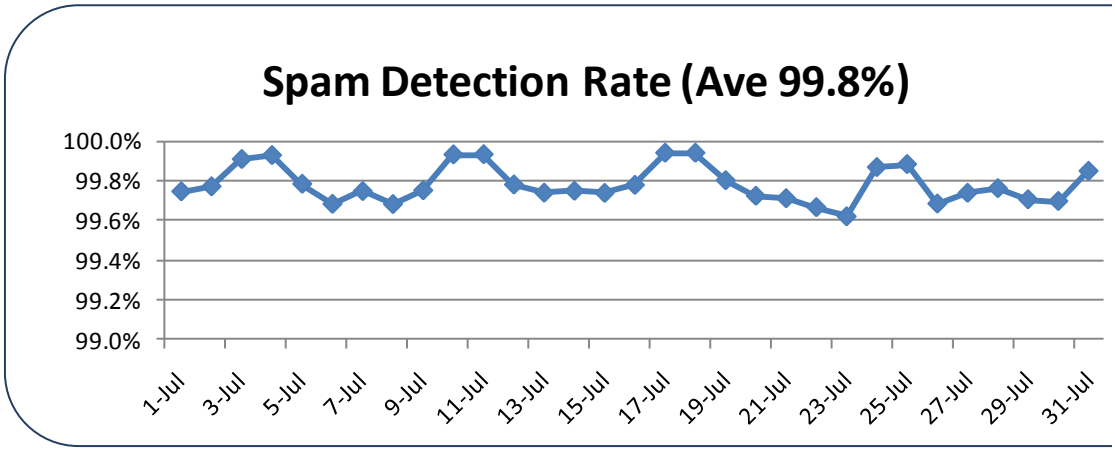

Figure 4 - Percent of spam detected (Average 99.8%)
This is evidence that we are consistently maintaining a very high spam detection rate. Customers should be very confident that with Websense they are receiving the best in anti-spam protection.

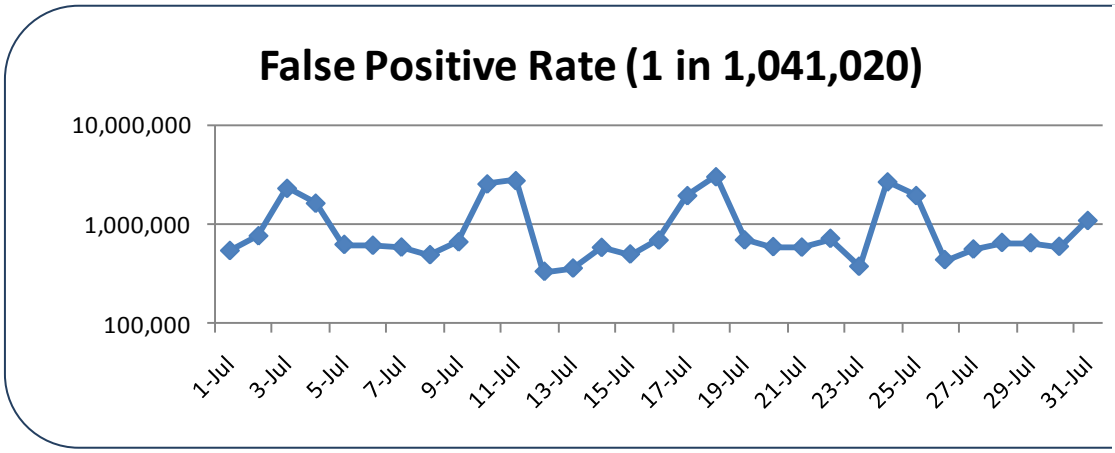

Figure 5 - False Positive Rate (Average 1 in 1,041,020)
This shows how Websense is consistently maintaining a very low false positive rate.
While Websense is catching a high percentage of spam, customers are rarely inhibited by messages falsely landing in a spam queue.

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.