

CRNtech

ELECTRONICALLY REPRINTED FROM MARCH 2009

ANTISPAM

Making Sense of E-Mail Threats

BY SAMARA LYNN



In light of all the ongoing, and terrible, security trends and case studies involving credit-card-number theft, bot attacks and remote execution of malicious code, e-mail spam seems more like a minor nuisance rather than an outright data threat by comparison.

Spam, however, is undeniably part of the threat landscape. Viruses can piggyback on it, but more often than not, spam can build up at exponential rates that may cost users hours in lost productivity as they attempt to rid their e-mail boxes of it.

Spam buildup can also be indicative of holes in a network's security defense. Spammers will often take advantage of open ports on misconfigured firewalls and SMTP servers to relay their annoying messages.

There are lots of products out there to combat spam. Many of them are bundled as all-in-one security solutions that include antimalware, firewall and Web filtering services. One such product is San Diego-based Websense Inc.'s Websense Hosted Security. Using Websense, traffic is filtered before reaching a customer's network. The vendor is so confident in its solution that a guarantee of 99 percent spam detection rate, 100 percent protection against known viruses, 99.999 percent service availability and no greater than 60 seconds for e-mail processing is offered with the Service Level Agreement.

CRN Test Center reviewers took a look at Websense Hosted Security via a remote, "hands-on" sandbox provided by the vendor. Although a hosted solution, Websense gives

a VAR or system administrator full control over the hosted protection environment. Web-based access of a remote management interface gives granular control over the system and provides information about the security well-being of a protected network.

The Dashboard contains both global and local information. The global is a display of information collected by Websense ThreatSeeker Network. During our demo, the top four globally reported e-mail viruses were Trojan-Dropper.Win32; Trojan-Spy.Win32.Zbo; W32/Dropper.AHGI; and Email-Worm.Win32.Net. This is a good way to find out what threat

is running amok most in cyberspace.

The ThreatSeeker Network uses a variety of security technology strategies to protect a client's network, including Websense reputation service, integrated Websense URL database, heuristics and fingerprinting.

Local information provided by the Dashboard gives a snapshot of internal data, such as Requests Processed and



the amount of bandwidth a customer's account has used in the last 7 days.

Granular control is evident in the Setup portion of the management interface. This is the area where user accounts are set up and directory synchronization (with Active Directory, for example) is configured. Even more extensive in configuration options are e-mail policies, which can be set so that notifications and messages are sent to senders and recipients, or both. Such a feature is often utilized by appending the company's e-mail security and confidentiality policy to all outbound mail. Websense makes it really easy to set up such a feature.

This is the area in the Web interface where administrators set rules governing the way antispam and antimalware filters handle inbound and outbound mail. There is even a setting to allow executables and scripts to pass through filters on a per-user basis (handy, perhaps, for the programmers and developers in an organization).

Content filtering frequently centers on how attachments are handled, but there is also another interesting feature—the ability to create lexical rules. A lexical rule compares words in a phrase or list to those in an e-mail and executes an action as specified by the administrator. Because lexical rules can be set against incoming and outgoing mail, companies can use it to prevent damning or potentially embarrassing information from leaving the company's network.

Other useful features include Native Reporting, Message Center and Audit Trail. Reports can be run to display a wealth

of information, such as details on e-mail volume, virus/malware statistics and account summaries. Message Center is a way to do advanced searching for messages. Audit trails allow the tracking and review of configuration changes that have taken place in an organization's hosted security account as well reviewing all quarantined items in an account.

Websense offers VARs not only a robust managed security solution, but an attractive newly revamped partner program. A new online channel partner locator will help North American customers find a Websense authorized solution provider. Enhanced Deal Registration is a way for partners to earn higher margins on standard and nonstandard new business deals. The vendor also has streamlined the renewal sales process via an online system that enables partners to efficiently manage subscription renewal as well as brand reports and customer communications on renewal activity. ■

Posted with permissions from the March 2009 issue of [CRNtech](#), United Business Media LLC. Copyright 2009. All rights reserved.
For more information about reprints from CRNtech, contact [Wright's Reprints](#) at 877-652-5295.



To evaluate Websense products,
visit www.websense.com