

And the solution? "Web filtering services are a powerful way to fight Bots, since users are blocked from suspicious web sites. Many IT administrators don't realise that, while they successfully fight the onslaught of inbound spam, their own systems may be compromised to the point of being the conduit for outbound spam and virus attacks. Comprehensive web filtering allows administrators to set specific access rules to web pages, based on the pages' categorised content."

BLENDING APPROACH

Typically, automatic updates to the URL database are done using various proprietary search algorithms to scour over web content looking for inappropriate or harmful content including malicious Bot Net sites.

"Our company's web filtering algorithms take a blending approach to categorising content, including scanning the target sites for viruses in setup files, zip files and executable files," adds Fertell. "If viruses are found, the site is added to one of our malware categories to prevent a seemingly harmless site from launching a drive-by install of malicious code or providing a fake hardware driver. There have been instances where we have identified over 10,000 such sites in less than a month."

Stopping malware at its source is often not the first approach his customers have tried, rather opting for retroactive anti-virus and spyware removal tools. "One of our healthcare customers was repeatedly being hit by open spam relays and viruses," he says. "Our Internet monitoring and filtering tools were deployed to stem the tide of constantly repairing their virus-stricken network. In addition, this hospital was able to identify where the problems were originating, in order to educate end users about downloading files with dangerous attachments." CS