



NewsFactor Network
Technology's Home Page

Anti-Spam Sites Hacked by Spammers

By James Maguire
NewsFactor Network
September 26, 2003

<http://www.newsfactor.com/perl/story/22374.html>



In an escalation of the battle between spammers and spam foes, two Web sites that post spam-blocking lists have been shut down by denial-of-service hack attacks. Additionally, an ISP that maintains an anti-spam list took the list offline after being harassed by hackers.

One of the sites, Monkeys.com, shut down this week after two recent DoS attacks. The initial bombardment, which lasted 10 days, was followed by a three-day attack. A second site, Osiriusoft.com, remains offline after a similar hack attack.

In response to continued hack attacks, sites that host spam-blocking lists are considering adopting P2P technology. Hosting the lists across a distributed network may make them less vulnerable to attack.

The third site, which is maintained by Tennessee-based ISP Compu-Net Enterprises, was taken offline after the ISP saw initial signs of an attack. Hackers sent e-mail falsely labeled to appear as if it originated from Compu-Net, and some valid mail was bounced.

"Our level of attack by the spammers had gone from nothing to massive," Bill Larsen, Compu-Net's administrator, told NewsFactor. "They were sending me a clear message that if I didn't do something, they were going to take action." || ||

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at +1 (818) 528-1100 or visit <http://www.newsfactor.com/about/reprints.shtml>.

Server in China

The three affected anti-spam sites are just a fraction of the hundreds that post spam-blocking lists. These so-called "black hole" lists contain the IP addresses of servers that are -- or may be -- used to route unsolicited junk e-mail.

Because ISP and other spam foes use these lists as part of their junk-mail filtering efforts, shutting down these sites is beneficial to those who profit from spam.

Industry experts cannot say with certainty who is perpetrating the recent attacks, but they suspect that professional spammers are responsible.

"There's a specific server in China that's sending out all the mail that's pretending to be from us," Larsen said. "Because it's in China, there's little or no recourse that we have."

SoBig vs. Anti-Spam Lists

Some analysts believe the recent SoBig virus was also an attempt to limit the effectiveness of the spam-blocking lists. Once SoBig infected a server, that machine could be used to route spam -- effectively circumventing the spam-block lists.

"Before the SoBig worm, we averaged less than 10 spam [messages] a day on public e-mails," Larsen said. "After SoBig it's gone up to close to 50, and for people who don't use these spam lists, it's probably more like 100 a day."

In response to continued hack attacks, sites that host spam-blocking lists are considering adopting P2P technology. Hosting the lists across a distributed network may make them less vulnerable to attack.

Spam Forecast

"The weather forecast is for continued spam for the foreseeable future," Aberdeen analyst Eric Hemmendinger told NewsFactor.

Although many forces are combating spam, "it continues to be a big moneymaker for people," added Forrester analyst Michael Rasmussen.

Federal anti-spam legislation is pending, and California this week passed a law that makes spammers liable for US\$1,000 per unsolicited e-mail and as much as \$1 million for a spam campaign. But the legislation "is unlikely to have an effect, because it doesn't take into account enforceability," Hemmendinger said.

And American legislation will have no effect internationally, Rasmussen told NewsFactor. "How do you pursue people who are out of the country?"

Avoiding E-Mail Harvesting

If IT administrators do nothing about spam, it will get worse, Hemmendinger said, adding that IT departments need to invest in filtering software or service. Additionally, since many spammers harvest addresses from Web sites, he recommended investing in products that make this more difficult.

"Until such time as [spammers] get prosecuted and face fairly stiff penalties," he noted, "there's not much of a disincentive." 

© Copyright 1998-2003 All rights reserved.

© Copyright 1998-2003 NewsFactor Network. All rights reserved.

This material may not be published, broadcast, rewritten or redistributed in any form without written permission. Please [click here for legal restrictions and terms of use](#) applicable to this site. Use of this site signifies your agreement to the terms of use. If you would like to reprint content from the NewsFactor Network, [click here](#) for pricing information. [Privacy Policy](#).
