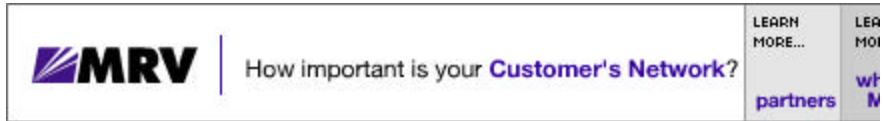




CRN
Vital Information
for VARs and
Technology
Integrators



MRV | How important is your **Customer's Network?**

February 16, 2004
Search:

CMP Channel Group


SUBSCRIBE NEWSLETTERS NETSEMINARS RESEARCH

FREE SUBSCRIPTION

MAIN:

- Home
- Breaking News
- This Week's CRN
- CRN Test Center
- Special Reports
- Broadcast News
- Top 25 Executives
- Industry Hall of Fame
- Columns

CRN RESEARCH:

- Research Home
- 25 Rising Stars
- Salary Survey
- Certification Study
- Channel Champions

NEWS CENTERS:

Select One:

SUBSCRIBER SERVICES:

- Customer Services
- Renew
- International Subs
- Back Issues

EDIT SERVICES:

- Meet the Editors
- Tip off ShadowRam
- Editorial Calendar
- Privacy Statement
- Media Kit
- Press Kit
- CRN Sales Contacts
- Strategy Guides
- International

CHANNELWEB NETWORK:

- Discussions
- Vendors Directory
- Career Center
- Sourcing Center
- Tools
- Resources
- Research

Breaking News

Poorly Guarded Home PCs Create Huge Spam Loophole

By [Anick Jesdanun](#), AP

4:10 PM EST Mon., Feb. 16, 2004

Next time you're looking for a culprit for all that junk mail flooding your inbox, have a glance in the mirror.

Spammers are increasingly exploiting home computers with high-speed Internet connections into which they've cleverly burrowed.

E-mail security companies estimate that between one-third and two-thirds of unwanted messages are relayed unwittingly by PC owners who set up software incorrectly or fail to secure their machines.

David Lawrence, 43, owns such a computer, which turned into a "spam zombie" when a virus infected it in October. Five or six spammers were using his cable modem to remotely send pitches for products like Viagra and boosters for cell phone signals.

"Spammers and the people who write these viruses ... is their life so void that they feel they have to mess up other people?" said Lawrence. "To me, it's criminal."

The self-employed businessman from Tifton, Ga., said he learned of his computer's culpability when his Internet service got suspended. "I called to find out what was going on because I knew I had the bill paid," he said.

Lawrence is by no means alone.

Hundreds of thousands of computers worldwide have been infected by SoBig and other viruses that are programmed to spawn gateways, known technically as proxies, to relay spam. Though Lawrence had antivirus software, he hadn't kept it updated.

It's ironic to the president of the security Web site myNetWatchman.com, Lawrence Baldwin, that those afflicted by spam are also often its couriers.

"That's further encouragement, justification for taking responsibility for your own

Join the discussion!
Talk Back

- [E-mail this article](#)
- [Print this article](#)
- [Link/reprint this article](#)

HOT LINKS

- ▶ [Security Software](#)
- ▶ [Janet Jackson Leads Web Searches, Spawns Spam](#)
- ▶ [Slamming Spam](#)

Breaking News

- ▶ [Poorly Guarded Home PCs Create Huge Spam Loophole](#)
- ▶ [Oracle Seeks To Mend Channel Woes With New Rules, Programs](#)
- ▶ [Security Guru: Microsoft Dominance Poses Huge Security Threat](#)
- ▶ [Thousands Of Records At Risk As Hackers Compromise California Server](#)
- ▶ [PeopleSoft Customers Want To Hear From Oracle](#)
- ▶ [Quantum Consolidates Channel Organizations](#)
- ▶ [Experts: Microsoft Code Leak Poses No Major Security Threat](#)
- ▶ [XO Wins Bidding For Allegiance Telecom Assets](#)

SEARCH

Search for more news about...

▶ [--Various--](#)

Get Mobilize



Monitor, manage and maintain your machines from virtually anywhere with Machine to Machine technology from Nokia.

M2M

[click here to join our community](#)

NOKIA
CONNECTING PEOPLE

How To Advertise
XChange Conferences
IPED
Digital Connect
Tech Builder

system," said Baldwin. "If you don't, you can be part of the very problem you're complaining about."

Any Internet-connected computer could be running a proxy spam relay, but most of the malicious programs are written specifically for PCs that run Windows.

In the past, some spammers had sought out and exploited Internet-connected computers with misconfigured networking software. The latest and growing threat is code purposely written to create spam relay proxies as it is spread by malicious viruses.

"It's just going to get worse," said Ken Schneider, chief technology officer at spam-filtering company Brightmail. "Traditionally, virus writers were driven more by reputation and trying to impress each other. Now there's an economic motive."

Just last week, a proxy program called Mitglieder began installing itself on computers infected by last month's Mydoom outbreak, said Mikko Hypponen, manager of antivirus research at F-Secure Corp. in Finland. He said such programs can also sneak in if computer owners fail to install patches to fix known Windows flaws.

The shift in spamming methods even prompted the Federal Trade Commission to issue a consumer alert last month. The advisory encouraged consumers to use antivirus and firewall programs and to check "sent mail" folders for suspicious messages.

Others say home users should also keep their Windows operating systems up to date by visiting [Microsoft's update Web site](#).

"If your computer has been taken over by a spammer, you could face serious problems," the FTC advisory wrote. "Your Internet Service Provider (ISP) may prevent you from sending any e-mail at all until the virus is treated, and treatment could be a complicated, time-consuming process."

In the early days, spammers sent out junk messages directly from their machines. ISPs easily found them and closed their accounts.

Spammers then looked for so-called open relays.

These are typically mail servers at ISPs, often in Asia or South America, carelessly configured so that anyone on the Internet can send mail through them without needing a password. The relays make messages appear to have come from an ISP, not the spammer.

But ISPs and anti-spam activists soon identified many of the open-relay machines and either pressured their owners to stop or blocked messages from them.

Stymied by a more concerted effort by ISPs to lock down their Internet mail servers, the spammers turned to the less vigorously protected home machines.

They are abundant and simple to find. Spammers can cover their tracks and become virtually untraceable.

"It pains me to say it, but it's very clever of the spammer to have thought of this, getting legitimate PCs to send spam on their behalf," said Andrew Lochart, director of product marketing at e-mail security company Postini.

Steve Atkins, chief technology officer at the anti-spam consultancy Word to the Wise LLC, said some ISPs continue to be plagued by open-relay techniques, but spammers generally don't bother with them anymore because it's so much easier



to have success with home machines.

Where much of the spam previously flowed through China, South Korea, Brazil and other countries whose ISPs left many relays open, it's now being hastened by a North American trend: more high-speed cable and DSL connections at home.

Such proxies are especially frustrating for ISPs to identify and block, said Mary Youngblood, abuse team manager at EarthLink Inc. She said some stay open only for a few hours and disappear by the time ISPs catch on, while newer ones reconfigure themselves constantly like chameleons on a single machine.

The more versatile the open proxy, the longer it takes to isolate.

John Levine, co-author of "Fighting Spam for Dummies," said the proliferation of proxies could force ISPs to take such measures as limiting how many messages a customer can send in a given time period.

In the meantime, ISPs are often being forced to cut off their own customers.

"As a customer, to have someone just arbitrarily shut me off, that would more than mildly displease me," said Walt Wyndroski, network operations manager for CityNet, which had shut down Lawrence. "We try to think from the customer's standpoint, but we also have to look at the larger view of the health of the network itself."

Copyright © 2004 The Associated Press. All rights reserved. The information contained in the AP News report may not be published, broadcast, rewritten or redistributed without the prior written authority of The Associated Press.

TalkBack

You can be the first to comment on this story !

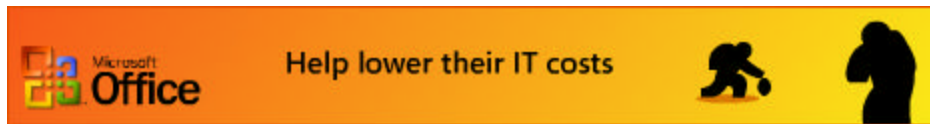
Start a New Thread

CMP Media LLC (CMP) and its sites: www.crn.com, www.varbusiness.com and www.channelweb.com provide Talk Back discussion boards as a professional medium for solution providers to discuss business problems. Gossip, personal attacks and unsubstantiated charges are prohibited.

Messages posted on this Web site as discussion threads or talkback (Content) are solely the opinions of their creators and do not necessarily reflect the opinions of CMP Media LLC (CMP) or its sites: www.crn.com, www.varbusiness.com and www.channelweb.com. All individuals who post material to this Web site are solely responsible for all Content that they upload, post or otherwise transmit via the Web Site.

CMP cannot vouch for the authenticity of the user or company names or e-mail addresses associated with posted messages. Messages are posted as is, that is they are neither edited for content nor checked for accuracy or authenticity. Under no circumstances will CMP Media LLC or ChannelWeb be liable in any way for any Content, including, but not limited to, for any errors or omissions in any Content, or for any loss or damage of any kind incurred as a result of the use of any Content posted or otherwise transmitted via the Bulletin Boards.

CMP reserves the exclusive right to edit or remove messages containing inappropriate language or other material that could be construed as libelous, potentially libelous, or otherwise offensive or inappropriate. Discussion forums, bulletin boards and chat facilities are provided by CMP solely for the convenience of those who make use of the service. CMP does not endorse the products and services or other offerings mentioned in messages.



[Privacy Statement](#) - [Copyright © 2004 CMP Media LLC](#) - [Terms of Service](#)