



## Sobig ... What's Next?

Just released: Race to prevent SobigF's weekend surprise underway. More info at <http://www.msnbc.com/news/955498.asp>

### Sobig.

- Named the fastest spreading virus of all time. (As of Thursday, MessageLabs Inc., which filters viruses from corporate E-mails, had intercepted more than 3 million messages carrying the malevolent payload.)
- First virus with the ability to auto update itself.
- On it's 6<sup>th</sup> revision. Future revisions build from all the already infected machines.
- First virus that sends out emails in clumps (batches, rather than one at a time). Making it faster & harder to stop.
- Sobig uses its own email software.
- Virus experts are warning computer users to prepare for the next variant that could arrive this weekend.

"This is the fastest email outbreak ever, both in sheer numbers and rate of infection," said Brian Czarny, MessageLabs. "At its peak, 1 in every 17 E-mails (intercepted by MessageLabs) contained the virus."

Experts speculate that Sobig could be the work of a virus writer employed by a spammer. If the E-mail attachment carrying the virus is opened, the application opens a back door that lets a hacker gain access without detection. Spammers use back doors to upload applications that send spam anonymously. Sobig propagates itself by "spoofing" E-mail addresses from an infected PC to send out more E-mails carrying the virus attachment.

At this point, from what we know and what we can extrapolate, the speculation is leading more toward spam (use) and the virus author generating revenue off Sobig. Virus authors working for spammers include an expiration date so others can't use the back door--and to ensure payment from their employers.

Sobig, which struck a week after a separate virus, dubbed Blaster, wreaked havoc among computer users globally, clogged company networks and flooded users' E-mail boxes with messages. America Online, for example, reported scanning 31 million messages containing E-mail attachments, three times the normal load. Of those, 13 million contained some type of virus, and 11.5 million carried the new Sobig worm.

### Fight Back against Viruses and Worms (For Business Systems) An ounce of prevention is worth a pound of cure.

1. Setup Microsoft Auto Updates for daily checks and updates (all Servers and Workstations)
2. Update your current antivirus program (yearly) & data files (daily)
3. Install a hardware Firewall (such as Watchguard, Cisco, Symantec, Sonic Wall, etc.)
4. Institute Corporate policies on email, train your users, configure workstation users without administrative rights.
5. Install a Spam Filter (such as Surfcontrol)

**What about email viruses?**  
Genesis' email systems caught & deleted 18,855 viruses last month! If you are hosting your email with Genesis, you never even saw them. If your email is hosted elsewhere, make sure they are scanned for viruses. Or move your email to Genesis.

---

**IMPORTANT NOTE:**  
**To continue receiving alerts and information, you must notify Genesis.**  
**Please complete and fax this to 239-337-4641.**

**Company:** \_\_\_\_\_ **Name:** \_\_\_\_\_

**Phone:** \_\_\_\_\_ **Fax:** \_\_\_\_\_

**Signature:** \_\_\_\_\_