

Sobig Lesson: Pay Attention to the E-Mail Gateway

Arabella Hallawell

The latest variant of the Sobig worm propagates via spamming techniques, and spammers have used the Sobig worm to send their e-mail messages. The best defense is to protect the enterprise at its boundary.

NEWS ANALYSIS

Event

On 22 August 2003, the Sobig.F worm attempted to connect to master servers, which the worm previously infected and controls. (The worm started spreading over the Internet on 18 August.) The worm retrieves an URL from which it downloads a Trojan horse file to the local computer. Then it executes the worm's main program. The program files could potentially steal confidential information and could contain additional malicious code. Of the 20 identified master servers, only one was not shut down and directed traffic to a porn site. However, the worm can update the master list of servers during the payload launch time. Sobig.F will deactivate and shut down on 10 September 2003.

Analysis

Sobig propagates using spammer techniques to trick e-mail recipients into opening messages, including the spoofing of sender addresses that are familiar to recipients. The second wave of the malicious code attack could have potentially unleashed a more potent payload in infected computers, but law enforcement, Internet service providers (ISPs), computer emergency response teams and security vendors mitigated the threat. Fortunately, the hijacked servers were based in North America and South Korea where ISPs and law enforcement have considerable leeway.

Spammers have used previous Sobig variants to get spam messages through. This blending of worms and spam indicate that spam — usually seen as a nuisance or legal risk — poses security risks, too. E-mail from spoofed addresses may not just be unwanted but may have attachments that contain malicious code. In response, enterprises should expand their security capabilities at the SMTP gateway. Like spam, worms such as Sobig succeed because e-mail inherently has weak authentication, and users have a permissive attitude toward messages that turn up in their mailboxes. Efforts by ISPs and carriers for more extensive blocking of addresses will help slow the flood of spam and stem e-mail as an easy vector for infection. Eventual standards for better authentication of e-mail will also help.

Recommendations:

Protecting against viruses requires more than traditional, regularly updated antivirus software:

- Check for and fix security holes on key servers and applications.
- Subscribe to security vulnerability alerts so that you can block ports and servers when indications of attacks are seen.
- Multiheaded threats like Sobig (and spammers) try to get past server-based antivirus controls. Add another layer of protection at the desktop with personal firewalls (especially for workers with broadband access).
- Examine SMTP server security hygiene to make sure these messaging servers cannot be hijacked and are not vulnerable to mass e-mail attacks.
- Turn off auto responses to outside recipients when viruses or spam are detected.
- Evaluate better trust models for e-mail, such as using signed e-mail or start to authenticate e-mail (for example, via challenge responses or lists of trusted external

senders). Mostly consumer ISPs use challenge responses for e-mail, but they are awkward for widespread enterprise use.

Analytical Source: Arabella Hallawell, Gartner Research

Recommended Reading and Related Research

- "Management Alert: The Need for E-Mail Security in a Growing Mobile World" — Enterprises considering a secure messaging solution should address six issues. **By Joyce Graff**
- "'SQL Slammer' Lessons: Traditional Antivirus Is Not Enough" — The successful management of malicious-code threats is a more-complex enterprise initiative than simply installing and maintaining antivirus software. **By Arabella Hallawell**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509