

Return of MyDoom Shows Need for Better Antivirus Response

Rich Mogull

The latest variant on the MyDoom worm was more annoying than destructive. But this new outbreak is a warning that we need to improve our responses.

NEWS ANALYSIS

Event

On 26 July 2004, a variant of the MyDoom worm spread rapidly throughout the Internet, clogging mailboxes and causing several major search engines to shut down or slow to a crawl.

Analysis

The havoc caused by the MyDoom variant underscores the continuing danger posed by viruses and worms. The e-mail that carried it was deviously drafted, and when the recipient opened the attachment and installed the virus, it automatically searched various Internet search engines for more addresses. This caused several major search engines to experience serious availability and performance problems.

For the most part, major virus outbreaks in recent years have not been overly destructive. However, security managers should be aware that this isn't always the case. In early July 2004, for example, a variant of the Lovgate worm resurfaced, but with a sinister difference: It replaced executable files on victims' hard drives with copies of itself, leaving victims' computers unable to run. In March 2004, the Witty worm inflected some 12,000 vulnerable computers in less than an hour, causing half of those systems to crash destructively. And although enterprises are generally well protected against virus and worm outbreaks, most consumers are extremely vulnerable or have already been compromised.

Recommendations: Gartner believes that viruses will continue to be mostly be an expense and annoyance to corporations. But security managers should also prepare for more destructive viruses by developing incident response plans to shield the enterprise and mass-restore their systems in the event of a destructive virus or zero-day infection. These plans should include:

- A shielding strategy in the event of an attack that takes advantage of a vulnerability for which no patch exists. Such a strategy should include shielding with firewalls, content filters/proxies and URL filters.
- Disabling or manual reconfiguring of vulnerable software or hosts (if possible) and monitoring of intelligence resources to detect activity before it hits the network.
- An isolation strategy to lock down network segments to control a spreading virus and support a safe environment to restore systems.
- Prioritization for restoration, cleaning and hardening. When a destructive event hits, it's essential to know what needs to be up and running first.
- Reversion to standard images in the short term for partial operations if disaster recovery plans for fully restoring systems fail.

Security managers should also deploy host firewalls and host intrusion prevention systems to provide protection while waiting for antiviral signatures.

Analytical Source: Rich Mogull, Gartner Research

Recommended Reading and Related Research

- "Hype Cycle for Information Security, 2004" — Evaluating the hype and the reality surrounding security is important for prudent investments and critical for properly protecting the enterprise at a reasonable cost. **By Vic Wheatman and others**

- "Cool Vendors in Security and Privacy" — Eleven cool vendors in IT security and privacy offer innovative technologies and products. **By Ray Wagner and others**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)

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