



Web SCO Diserang MyDoom

Kejutan awal 2004 ini cukup mencengangkan, karena beredarnya satu jenis virus, yang dibuat secara spesifik menyerang web SCO pada 26 Januari 2004 yang lalu. SCO menyediakan hadiah US\$330.000 bagi yang menemukan pembuat virus itu, dan US\$250.000 hadiah juga ditawarkan oleh Microsoft.

Virus yang ditenggarai berasal dari Rusia ini belum bisa dicari sumbernya, walaupun beberapa perusahaan antivirus sudah menemukan obatnya. Virus yang dikenal dengan nama MyDoom, Novarg, atau variasi dari virus Mimail, juga menyerang *mail server* dan menyebarkan e-mail dengan subjek "Mail Delivery System," "Test" atau "Mail Transaction Failed." Isi e-mail-nya adalah file yang langsung dijalankan dan berisi keterangan: "The message contains Unicode characters and has been sent as a binary attachment."

Virus ini menyerang e-mail server pada sekitar tanggal 26 sampai 29 Januari 2004, dengan isi tulisan "The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment." Hampir ribuan e-mail masuk ke mailbox pemakai Internet, termasuk mailbox penulis yang menerima lebih dari 2.000 e-mail hasil kerjaan varian virus MyDoom.

Diduga ada pengguna Linux yang membenci SCO karena pada tahun lalu mengirim surat kepada lebih dari 1.500 perusahaan pembuat distro Linux untuk menghentikan penyaluran distronya dengan alasan melanggar hak cipta yang dimiliki SCO. Dalam beberapa mailing list Linux, banyak yang membantah isu ini, walaupun dalam beberapa kondisi memang mengarah ke dugaan tersebut.

Sampai tulisan ini dibuat, www.sco.com masih belum dapat diakses, karena efek dari virus tersebut cukup membuat bingung para teknisi SCO. Serangan terhadap SCO ini merupakan yang kedua kali dalam kurun waktu kurang dari dua bulan. Pada 10 Desember 2003, web SCO diakses lebih dari 700 juta "pengunjung" dalam waktu 32 jam, yang menyebabkan kerja komputer menjadi sangat lambat, serta *bandwidth* habis dipakai virus yang menyerang *web server* SCO terus menerus. Lebih dari seminggu web SCO tidak dapat diakses, sampai SCO memanggil dinas rahasia Amerika untuk mencari pembuatnya.

Efek virus MyDoom tidak hanya menyerang web SCO, tetapi juga pengguna program *e-mail client* di Microsoft Windows (Outlook Express). Telah ditemukan varian-varian yang cukup berbahaya. Virus masuk ke sistem Windows, lalu membuat penyerangan yang tersembunyi sehingga sulit dilacak dari mana asal virus tersebut. Di <http://www.microsoft.com/security/antivirus/mydoom.asp> dijelaskan bagaimana mendeteksi virus ini dengan cara yang sederhana, yaitu dengan menggunakan perintah `/a /s` di prompt DOS.


Yang meraup untung dalam kasus ini adalah para pembuat antivirus yang berlomba-lomba untuk membuat penangkal MyDoom, seperti McAfee, F-Secure, Sophos, Kaspersky Labs dan Trend Micro, di samping ada iming-iming dari Microsoft dan SCO. Pemberian hadiah untuk pemberitahu pembuat virus ini bukan untuk kali pertama dilakukan Microsoft, karena pada bulan November 2003 Microsoft juga menawarkan hadiah US\$250.000

untuk penemu pembuat virus SoBig dan Blaster.

Tetapi sampai akhir Januari lalu, belum ada perorangan atau perusahaan yang dapat menunjukkan pembuat virus-virus ganas ini, sehingga ada anggapan bahwa komunitas bawah tanah pembuat virus ini sangat loyal dan

tidak akan membocorkan rahasia mereka, walaupun sudah banyak yang mengetahui siapa pembuat virus tersebut.

Dengan adanya media-media jaringan komputer umum, seperti warnet (Internet Café), jaringan *wireless* dan komputer yang dipakai untuk melakukan penyebaran, maka akan sangat sulit untuk mengetahui dengan tepat siapa pembuat dan penyebar virus-virus tersebut, kecuali ada komunitas atau kawan-kawan seperjuangannya yang membelot dan memberitahukan ke media massa.

Pembuat MyDoom masih dicari, walaupun banyak pihak tidak begitu yakin bisa menemukan pembuatnya. Karena virus dengan besar hanya 28 KB ini mampu membuat varian-varian lain yang di masa mendatang akan lebih ganas lagi. Kemampuannya membuka port 3127 dan 3198 dari Microsoft Windows membuat penyebarannya lebih intensif dan merata. Berbahagialah para pemakai Linux, karena sepertinya masih aman dari serangan virus-virus ini. 

MyDoom tidak hanya menyerang web SCO, tetapi juga pengguna program e-mail client di Microsoft Windows (Outlook Express).