Komponen Penting di Tubuh Virus (Dari Pandangan Protagonis)

ÇäkrabiRâwÄ
Depok - Indonesia
Cakrabirawa@mail.ru
http://come.to/digitalworks

Tulisan ini pernah dimuat di Tabloid PCplus No. 82 – 83 Th. III, Juni 2002

Dalam artikel ini penulis akan menjelaskan mengenai komponen yang menyusun tubuh virus dari sudut pandang protagonis. Tujuannya hanya satu yaitu menjelaskan bagian – bagian virus secara lebih jelas dan mengena, sehingga sudut pandang yang dipakai adalah sudut pandang dari para pembuat virus. Semoga memperluas wawasan pembaca mengenai virus komputer.

Setiap virus mempunyai bagian – bagian atau biasa disebut *routine*. Bagian – bagian yang menyusun virus ada yang penting yang mesti ada pada "seekor" virus dan ada juga yang bersifat tambahan. Komponen tambahan ini meski tidak begitu penting tetapi tetap menjadi karakteristik yang membedakan satu virus dengan virus yang lainnya.

Pada atikel ini penulis akan menjelaskan dua komponen yang mendasar yang berperan penting dalam kelangsungan hidup virus, yaitu dalam hal meloloskan diri dari "seleksi alam". Komponen tersebut mesti ada pada setiap virus. Komponen – komponen tersebut adalah *search routine* (rutin pencari) dan *copy routine* (rutin pengganda). Satu rutin lagi yaitu *anti detection routine* merupakan komponen tambahan saja. Tetapi meski bersifat tambahan tetap mempunyai arti penting dalam kelangsungan hidup virus untuk berkelit dari "predator" – nya.

Rutin Pencari

Rutin pencari (*search routine*) ini berperan sebagai unit yang mencari file – file baru atau daerah (area) baru pada disk yang nantinya akan diinfeksi. Rutin ini erat kaitannya dalam menentukan seberapa baik virus akan bereproduksi. Apakah dia akan bereproduksi secara cepat atau lambat. Termasuk juga menentukan seberapa banyak disk yang akan diinfeksi dan juga daerah – daerah tertentu pada disk yang akan menjadi target penginfeksian. Semakin rumit rutin pencarinya maka semakin besar rutin pencarinya. Semakin handal rutin pencarinya maka akan sangat membantu dalam penyebaran virus.

Rutin Pengganda

Komponen yang kedua yang harus dimiliki oleh "seekor" virus adalah rutin pengganda. Rutin ini berfungsi untuk meng – copy virus ke suatu area yang telah ditentukan oleh rutin pencari. Ukuran besar kecilnya rutin pengganda ini tergantung juga dari kekomplekan virus dalam meng – copy – kan dirinya. Sebagai contoh, virus yang menginfeksi file COM akan mempunyai rutin pengganda yang lebih kecil dari virus yang menginfeksi file EXE. Hal ini dikarenakan struktur file EXE lebih rumit ketimbang file COM, sehingga banyak yang harus dilakukan virus untuk dapat menempel ke file EXE.

Rutin Anti Deteksi

Untuk dapat mencapai tujuannya yaitu mampu mencari file induk yang akan diinfeksi dengan rutin pencari dan kemudian menginfeksinya dengan bantuan rutin pengganda, virus juga membutuhkan fitur – fitur tambahan. Fitur – fitur ini akan sangat berperan dalam mendukung tujuan tersebut. Diantara fitur yang biasanya ditambahkan dalam tubuh virus adalah rutin untuk menghindari deteksi. *Anti detection routine* ini berperan dalam menghindari deteksi baik dari pengetahuan user atau dari pantauan program anti virus yang memang merupakan *predator* – nya. *Anti detection routine* bisa saja dibangun menyatu dengan rutin pencari atau rutin pengganda sehingga menjadi bagian yang integral. Tetapi bisa juga merupakan bagian yang tersendiri.

Kerja rutin pencari ini haruslah dibatasi untuk menghindari deteksi. Maksudnya bila rutin pencari bekerja terus – menerus memeriksa setiap file yang ada dalam disk, maka akan membutuhkan waktu yang lama dan menyebabkan aktifitas disk yang tidak normal dan tidak biasa. Ini tentu cukup mengkhawatirkan karena seorang user yang cukup waspada dengan aktifitas virus bisa menjadi curiga, dan keberadaan virus dapat diketahui. Hal ini tentu sangat tidak diinginkan oleh para pembuat virus karena kelangsungan hidup virus menjadi terhambat.

Sebagai alternatifnya untuk mendukung *anti detection routine*, virus diaktifkan pada kondisi – kondisi tertentu. Misalnya pada tanggal – tanggal tertentu. Contohnya adalah virus – virus dari keluarga Friday 13. Virus ini merupakan virus parasitik yang berbahaya dan bekerja dengan mencari seluruh file – file yang berekstensi .COM (kecuali COMMAND.COM) pada direktori aktif berikut sub direktorinya. Kemudian menempelkan dirinya pada bagian akhir file korban. Virus ini aktif setiap hari Jum'at ketiga belas dengan menghapus file – file.

Ada juga virus yang menggunakan alternatif yang lainnya, misalnya dengan mendeteksi hentakan keyboard. Bila keyboard tidak ditekan selama sekian menit (misal 10 menit), maka virus mulai diaktifkan. Trik ini termasuk cukup "cerdik" untuk memastikan bahwa seorang user benar – benar tidak sedang berada di depan komputernya. Sehingga aktifitas virus yang menunggangi operasi komputer dapat berjalan lancar tanpa sepengetahuan user.

Rutin pencari, pengganda dan anti deteksi merupakan komponen – komponen yang mendasar yang ada dalam setiap virus. Tentu saja virus – virus komputer mempunyai rutin – rutin tambahan yang lain disamping ketiga rutin tersebut, dengan tujuan untuk menghentikan operasi normal komputer, untuk menyebabkan kerusakan

atau bisa juga sekedar *joke* (hiburan) yang menyenangkan bagi pemrogram virusnya tetapi bagi orang lain bisa membuat jantung berdebar hebat. Rutin – rutin tersebut akan mempengaruhi karakter "seekor" virus dan juga berperan penting dalam mencapai tujuan virus yaitu kelangsungan hidup dan bereproduksi. Bila saja hanya sedikit aktifitas disk maka tidak ada orang yang akan memperhatikan dan keberadaan virus tidak akan diketahui. Lain halnya dengan virus – virus yang banyak menarik perhatian orang dengan menampilkan kotak dialog "salam" atau dengan langsung menimbulkan kerusakan pada disk saat itu juga, sehingga orang awam pun bisa langsung menebak keberadaan virus di komputernya. Sehingga virus dengan cepat dapat dibasmi. Virus tersebut tidak lolos "seleksi alam".

Virus – virus yang tidak mementingkan kelangsungan hidupnya lebih berperan sebagai perangkat "delivery system" saja. Pembuatnya tidak peduli apakah virus tersebut akan musnah di dalam aksinya ketika virus telah mencapai sasarannya. Virus mirip dengan pilot Kamikaze yang mengorbankan hidupnya untuk menyelesaikan sebuah misi. Dalam masalah ini virus dapat menjadi sebuah perangkat militer yang cukup efektif untuk menyelesaikan sebuah **misi**.