Mengenal Virus pada File Dokumen

Oleh Adi Sumaryadi

Istilah "Banyak Jalan menuju ke Roma" atapun "Tak ada tali akarpun jadi" sepertinya saat ini tidak hanya dapat dipergunakan oleh manusia saja, tetapi viruspun sudah menggunakan istilah ini dalam penyebarannya. Pembuat virus sepertinya tidak kehabisan akal untuk mencari jalan baru untuk melakukan serangan kepada komputer korban atau sistem jaringan yang menjadi target. Salah satu jalan yang ditempuh adalah dengan memanfaatkan file dokumen yang hampir setiap pengguna komputer menggunakannya setiap menyalakan komputer. Modus pemanfaatan dokumen itu sendiri dilakukan dengan melakukan penyamaran sebagai file dokumen atau menyisipkan di file dokumennya itu sendiri.

Istilah "Banyak Jalan menuju ke Roma" atapun "Tak ada tali akarpun jadi" sepertinya saat ini tidak hanya dapat dipergunakan oleh manusia saja, tetapi viruspun sudah menggunakan istilah ini dalam penyebarannya. Pembuat virus sepertinya tidak kehabisan akal untuk mencari jalan baru untuk melakukan serangan kepada komputer korban atau sistem jaringan yang menjadi target. Salah satu jalan yang ditempuh adalah dengan memanfaatkan file dokumen yang hampir setiap pengguna komputer menggunakannya setiap menyalakan komputer. Modus pemanfaatan dokumen itu sendiri dilakukan dengan melakukan penyamaran sebagai file dokumen atau menyisipkan di file dokumennya itu sendiri.

Kenapa Mesti Dokomen?

Hampir semua komputer yang ada saat ini pasti terpasang aplikasi Office Suite seperti Microsoft Office ataupun Program Office lainnnya, hal ini terjadi karena rata-rata komputer rumahan dan komputer perkantoran digunakan untuk memproses dokumen, baik hanya dokumen text sederhana maupun dokumen yang rumit. Hal inilah yang dimanfaatkan oleh para pembuat virus sebagai jalan masuknya virus kekomputer korban atau merusak file dokumennya itu sendiri. Kecerobohan dan ketidaktauan pengguna juga menjadi jalan emuk untuk sebuah virus dalam menjalankan seranganmya. Selain dari sering digunakan, file dokumen juga memiliki ukuran yang kecil-kecil, apalagi didokumen tersebut tidak disisipi gambar. Dengan ukuran yang sangat kecil file-file dokumen akan sangat mudah ditransfer kesana kemari baik menggunakan media online ataupun harddrive seperti flashdisk dan disket.

Mobilitas file dokumen yang sangat tinggi inilah yang dimanfaatkan oleh pembuat virus untuk lebih gencar melakukan penyebaran virus, sebagai contoh seorang mahasiswa membuat satu dokumen tugas akhir, secara tidak tau dokumen tersebut disisipi virus yang membahayakan, karena merasa aman, file dokumen tugas akhir digunakan teman-temannya sebagai contoh, alhasil file tersebut sangat cepat menyebar dan menyebar.

Adalah virus Kangen yang mempunyai kemiripan dengan virus Pesin dengan beberapa perbedaan kecil. Sama seperti Pesin atau MyHeart, Kangen menyebar melalui disket dan jaringan (File Sharing) dan akan membuat file yang mengandung virus mirip dengan dengan icon file dokumen Microsoft Word dengan ekstensi EXE (executable). Dalam menyebarkan dirinya melalui jaringan (file sharing), Kangen tidak dapat berjalan secara otomatis melainkan memerlukan bantuan pihak ketiga untuk menjalankan file yang telah terinfeksi. Dengan modus penyamaran sebagai file Microsoft Word dengan nama file kangen, maka orang awam bisa saja langsung mengklik dan secara otomatis akan menjalankan virus tadi, munculah aplikasi microsoft word yang berisikan lagu kangen milik Dewa 19 sebagai tanda bahwa komputer tersebut telah terinfeksi dan siap menerima akibatnya.

Virus Dokumen yang paling sepuh adalah virus macro yang terdapat di file Dokumen, walaupun virus ini saat ini tidak terlalu berbahaya, namun keberadaannya terkadang sangat menyebalkan, oleh karena itu vendor-vendor pembuat aplikasi Office Suite selalu menyertakan antivirus internal yang mendeteksi keberadaan virus ini sebelum dokumen dibuka.

Kenali Karakateristiknya

Banyaknya jenis virus komputer yang ada semakin banyak pula karakteristik yang terdapat pada masing-masing virus. Untuk jenis virus yang berhubungan dengan dokumen biasanya beraksi dengan menyamar diri menjadi file documennya itu sendiri, misalkan dengan memasang icon microsoft word pada dirinya sehingga korban mudah tertipu karena sebenarnya file tersebut bukan word asli melainkan exe. Virus penyerang dokumen biasanya mempunyai ukuran file yang kecil-kecil, hal ini kemungkinan untuk mempermudah penyebaran, ukuran file virus penyerang dokumen tidak lebih dari 100 Kilobytes. Tipe infeksi yang sering dilakukan biasanya menghidden file dokumen yang kita punya atau merusak isi dari dokumen itu sendiri, yang paling berhaya adalah ketika virus melakukan penghapusan file dokumen. Virus penyerang dokumen biasanya akan selalu menggandakan dirinya setelah komputer korban terinfeksi, hal pertama yang dilakukannya adalah mematikan service-service yang ada dimemory sehingga service tadi tidak menghapusnya. Hal yang paling berbahaya adalah ketika virus selalu melakukan restart terhadap sistem, jika kejadian ini terjadi berulang ulang akan menyebabkan harddisk crash dan tidak bisa digunakan lagi.

Tindakan Preventif

Menjadi sebuah keharusan jika anda pengguna Microsoft Windows untuk selalu memasang antivirus dikomputer anda, tetapi jangan merasa nyaman dulu jika antivirus anda jarang diupdate, oleh karena itu updating antivirus akan sangat membantu anda dalam menangkal atau menghindari virus-virus terbaru. Hal lain yang harus dilakukan adalah sikap kehati-hatian kita yang harus ditingkatkan, ketika kita mengcopy file dari tempat-tempat umum seperti laboratorium, warnet atau komputer teman, pastikan tidak ada virus yang ikut didalamnya dengan melakukan scanning terlebih dahulu atau melihat secara fisik file-file yang ada didalamnya. Andai saja komputer anda terlanjur sudah terinfeksi, maka yang harus anda lakukan adalah dengan mencari removalnya jika antivirus yang anda miliki tidak bekerja atau dengan berkunjung ke website-website yang menyediakan panduan penghapusan virus tertentu.

Kata Kunci :