Virus Malware
Jum`at, 19 Juni 2015 | 23:23:49 WIB **| Endang Kurniawan**

Menurut para ahli virus, penjelasan tentang malware dan virus selama ini belum sepenuhnya bisa memenuhi dasar ilmiah untuk klasifikasi malware/virus sehingga terbawa pemahaman virus cenderung pada virus dalam arti ilmu biologi, padahal ini virus computer bukan pada bidang biologi tetapi mirip gaya bahasa personifikasi terhadap virus memang meniru pemahaman pada biologi atau mendekati pada bidang kedokteran, bagi awam masyarakat luas memang lebih mudah menerima virus seperti di bidang kedokteran sehingga kengerian akan virus computer benar-benar serasa berbahaya seperti virus kedokteran.

Virus computer hanyalah sebuah progam, sama dengan progam computer lainnya, begitulah cara memudahkan pemahaman awal virus, dalam aplikasinya terpecah jadi program jahat (virus) dan progam baik dimana si jahat melengkapi kemampuannya seperti penjahat dengan sifat menyerang secara tersembunyi, merusak program baik, menonjolkan ideologi jahat programernya dan ingin terkenal dengan cara-cara jahat, secara outomatis hal ini membangkitkan perlawanan dari program baik berbentuk “Anti-Virus” yang akhirnya keduanya berhadapan saling menghancurkan satu sama lain, mirip kehidupan manusia melawan kejahatan, untuk pelaku kejahatan disebut Cracker dan sisi baiknya disebut Hacker. Virus yang sudah ditangkap karena terbukti bersalah lalu diperiksa cara operasi kejahatannya sehingga kita bisa mengenali karakteristik virus tersebut, disini ada khas humanis yaitu “tidak bisa ditangkap sebelum terbukti bersalah”, disini sempat membuat programer ‘Anti-Virus” jadi paranoid karena diganggu sifat program jahat tetapi tidak ada bukti dan tidak ada korbannya.

Kata virus hampir selalu dipakai untuk menyebut program-program yang sengaja dibuat agar dapat merusak komputer tanpa sepengetahuan pemilik komputer. Suatu program dapat disebut sebagai suatu virus apabila memenuhi minimal 5 kriteria berikut :

1. Kemampuan untuk mendapatkan informasi.

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory. Untuk apa? Agar dia dapat memperoleh daftar file yang bisa dia tulari.

Misalnya, virus makro yang akan menginfeksi semua file data MS Word, akan mencari daftar file berekstensi *.doc. Disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/data semua file, lalu memilahnya dengan mencari file-file yang bisa ditulari. Biasanya data ini tercipta saat file yang tertular/terinfeksi virus atau file program virus itu sendiri dibuka oleh user. Sang virus akan segera melakukan pengumpulan data dan menaruhnya (biasanya) di RAM, sehingga apabila komputer dimatikan semua data hilang.

Tetapi data-data ini akan tercipta kembali setiap kali virus itu diaktifkan. Biasanya data-data ini disimpan juga sebagai hidden file oleh virus tersebut.

2. Kemampuan untuk memeriksa suatu file.

Suatu virus juga harus bisa memeriksa suatu file yang akan ditulari, misalnya dia bertugas menulari program berekstensi *.doc, maka dia harus memeriksa apakah file dokumen tersebut telah terinfeksi ataupun belum, karena jika sudah, akan percuma menularinya lagi. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program. Yang umum dilakukan oleh virus adalah memiliki/memberi tanda pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut.

Contoh penandaan adalah misalnya memberikan suatu byte yang unik di setiap file yang telah terinfeksi.

3. Kemampuan untuk menggandakan diri dan menularkan diri.

Kalau ini memang virus “bang-get”, maksudnya, tanpa kemampuan inii tak adalah virus. Inti dari virus adalah kemampuan mengandakan diri dengan cara menulari file lainnya. Suatu virus apabila telah menemukan calon korbannya maka ia akan mengenalinya dengan memeriksanya. Jika belum terinfeksi maka sang virus akan memulai aksinya penularan dengan cara menuliskan byte pengenal pada file tersebut, dan seterusnya mengcopikan/menulis kode objek virus diatas file sasaran.

Beberapa cara umum yang dilakukan oleh virus untuk menulari/menggandakan dirinya adalah :

- File yang akan ditulari dihapus atau diubah namanya. Kemudian diciptakan suatu file berisi program virus itu sendiri menggunakan nama file yang asli.
- Program virus yang sudah dieksekusi/load ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file yang ada.

4. Kemampuan melakukan manipulasi.

Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulari suatu file. Isi dari suatu rutin ini dapat beragam mulai dari yang tidak berbahaya sampai yang melakukan perusakan. Rutin ini umumnya digunakan untuk memanipulasi file atau pun mempopulerkan pembuatnya ! Rutin ini memanfaatkan kemampuan dari suatu sistem operasi (Operating System), sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem operasi.

Misal:

- Membuat gambar atau pesan pada monitor.
- Mengganti/mengubah-ubah label dari tiap file, direktori, atau label dari drive di PC. Memanipulasi file yang ditulari.
- Merusak file.
- Mengacaukan kerja printer, dsb.

5. Kemampuan untuk menyembunyikan diri.

Kemampuan menyembunyikan diri ini harus dimiliki oleh suatu virus agar semua pekerjaan baik dari awal sampai berhasilnya penularan dapat terlaksana.

Jenis-jenis Malware :

- Logic Bomb
- Trojan Horse
- Back Door
- Virus Worm
- Rabbit
- Spyware
- Adware
- Hybrids, Droppers, and Blended Threats
- Zombies

Sumber : https://endangkurniawan.com/article-virus-malware.html