Mengenal Berbagai Jenis Malware dan Pencegahannya

Oleh: Mochammad Firdaus Agung

Malware atau Malicious Software merupakan sebuah serangan infeksi digital yang saat ini dirasa paling populer di kalangan pengguna internet dunia termasuk di Indonesia. Malware mampu masuk ke dalam sistem komputer dan melakukan aktivitas yang merugikan bagi pengguna komputer.

Kerugian yang ditimbulkan dari kehadiran Malware sangat beragam, mulai dari memperlambat kerja sistem komputer, merusak atau menghilangkan data hingga mampu memberikan perintah kepada komputer yang telah terinfeksi Malware dari jarak jauh (Remote Access).

Diharapkan dengan mengenal berbagai jenis Malware dapat membuat kita semakin sadar akan bahaya yang ditimbulkan dari kehadiran Malware di komputer kita. Pengenalan terhadap Malware ini membuat kita mampu untuk sedikit mengerti mengenai dampak yang akan timbul terhadap suatu jenis Malware bila sudah menginfeksi sebuah sistem komputer.

Berikut ini akan dijelaskan berbagai jenis Malware yang dinilai paling dominan menginfeksi komputer di Indonesia:

1. Virus

Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah Malware pertama yang dikenalkan sebagai program yang memiliki

kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah Malware sendiri.

Biasanya virus berbentuk file eksekusi (executable) yang baru akan beraktivitas bila user mengaktifkannya. Setelah diaktifkan virus akan menyerang file yang juga bertipe executable (.exe) atau juga tipe file lainnya sesuai dengan perintah yang dituliskan pembuatnya. Hingga disadari kehadiran virus sangat mengganggu dan membuat banyak perusahaan yang tertarik untuk melakukan development dengan membuat Anti Virus yang nyatanya memang laku keras di pasaran.

2. Worm

Worm yang berarti cacing merupakan Malware yang cukup berbahaya. Worm mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, Worm memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di dalam sistem komputer.

Hal yang diakibatkan dari aktivitas Worm adalah merusak data dan memenuhi memory dengan Worm lainnya hasil dari penggandaan diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan komputer menjadi hang dapat menjadi gejala awal terdapatnya Worm pada komputer tersebut.

Contoh Worm yang populer akhir-akhir ini adalah Conficker yang memanfaatkan celah keamanan pada RPC (menggunakan port 445) di komputer bersistem operasi Windows

3. Trojan Horse

Teknik Malware ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke Hollywood dalam film berjudul ‘Troy’. Modus dari Trojan Horse ini adalah menumpangi file biasa yang bila sudah dieksekusi akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama file yang ditumpanginya.

Trojan Horse merupakan Malware berbahaya, lebih dari sekedar keberadaannya tidak diketahui oleh pengguna komputer. Trojan dapat melakukan aktivitas tak terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan file, mencuri data, melihat aktivitas user (spyware), mengetahui apa saja yang diketikkan oleh user termasuk password (keylogger) bahkan menguasai sepenuhnya komputer yang telah terinfeksi Trojan Horse.

Dalam perkembangannya Teknik Trojan Horse telah dimanfaatkan oleh program Botnet (Robot Network) yang akan menjadi sangat berbahaya bila berhasil masuk ke dalam komputer yang memiliki koneksi jaringan dengan komputer lainnya secara luas. Penanganan

terhadap Botnet menghadapi permasalahan yang sangat kompleks dan terus dipelajari hingga sekarang.

4. Spyware

Spyware merupakan Malware yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan Spyware jelas sangat merugikan user karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya.

Aktivitas Spyware terasa sangat berbahaya karena rentan terhadap pencurian password. Dari kegiatan ini juga akhirnya lahir istilah Adware yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. Spam yang muncul secara tak terduga di komputer juga merupakan salah satu dampak aktivitas Spyware yang dirasa sangat menjengkelkan.

5. Backdoor

Kerja dari Backdoor sangat berkaitan dengan aktivitas hacking. Backdoor merupakan metode yang digunakan untuk melewati autentifikasi normal (login) dan berusaha tidak terdeteksi. Backdoor sendiri sering kali disusupkan bersama dengan Trojan dan Worm. Dapat diartikan secara singkat Backdoor berarti masuk ke sistem komputer melalui jalur pintu belakang secara tidak sah.

Dengan metode Backdoor maka akan sangat mudah untuk mengambil alih kendali dari komputer yang telah berhasil disusupi. Setelah berhasil masuk maka aktivitas yang dilakukan oleh Backdoor antara lain adalah mengacaukan lalu lintas jaringan, melakukan brute force attack untuk meng-crack password dan enkripsi dan mendistribusikan serangan Distributed Denial of Service (DDoS).

Pencegahan Infeksi Malware

Setelah disadari betapa berbahayanya Malware ketika sudah berhasil masuk ke dalam suatu sistem komputer. Maka dibutuhkan suatu kegiatan yang lebih dari sekedar pengetahuan mengenai Malware. User menjadi tokoh sentral dalam menghindari terjadinya infeksi Malware di komputernya.

Hampir secara keseluruhan dapat disimpulkan bahwa Malware hanya akan memulai aktivitasnya bila User mengaktifkannya terlebih dahulu. Sekalipun ada Malware yang langsung menyebar otomatis seperti Worm. User diharapkan untuk sangat berhati-hati dan memiliki sikap waspada sebelum mengaktifkan / mengklik sesuatu yang dirasa asing.

Bahaya Malware sangat besar karena terus berinovasi seiring kemajuan teknologi. Saat ini Malware telah berbentuk menjadi simbol Folder atau menyamar dengan bereksstensi file

yang sudah familiar di kalangan user seperti .jpg, .doc, .txt dan sebagainya yang secara kasat mata dinilai sebagai file biasa namun bila diklik akan menjalankan aktivitas yang berbahaya.

Penyebaran Malware semakin tak terkendali dengan hadirnya internet yang membuat Malware semakin mudah menyebar terutama melalui website penyedia fasilitas file sharing. Kebiasaan di kalangan masyarakat Indonesia untuk berbagi file menggunakan media flashdisk juga sangat rentan dengan ancaman Malware.

Flashdisk sendiri saat ini menjadi tempat empuk bagi Malware untuk menyebar dan masuk ke sistem komputer. Entah secara disengaja atau tidak namun untuk mencegah penyebaran Malware ada baiknya untuk mulai bersikap selektif terhadap penggunaan flashdisk. User diharapkan untuk waspada dengan tidak sembarangan berbagi file melalui flashdisk dengan orang yang kurang dikenal.

Pemasangan Anti Virus di komputer juga sangat dianjurkan selain juga pengaktifan Firewall yang biasanya sudah aktif dalam kondisi default. Penggunaan Anti Virus juga harus selektif karena saat ini malah banyak Anti Virus yang ditumpangi oleh program Malware. Update Anti virus secara berkala juga sangat penting untuk mulai dibiasakan.

Penggunaan Sistem Operasi dan Software yang selalu update juga dapat menghindari serangan Malware. Bila komputer selalu diperbarui versi programnya maka Malware akan sulit untuk beradaptasi melakukan serangan. Tentunya update dilakukan di tempat yang terpercaya dan juga komputer menggunakan produk software yang asli dan bukan bajakan yang didapatkan dari sembarang tempat.

Kegiatan pencegahan lainnya yang lebih bersifat antisipasi adalah melakukan backup data. Melalui kegiatan backup data maka kita memiliki cadangan data yang sama seperti yang ada di komputer namun disimpan di tempat lain di luar komputer, disimpan di harddisk eksternal misalnya. Backup data membuat kita masih memiliki data cadangan apabila data pada komputer mengalami kerusakan atau hilang yang disebabkan oleh infeksi Malware.

Beralih menggunakan sistem operasi open source juga dapat menjadi solusi cerdas. Selain untuk menghindari Malware, sistem operasi open source juga didapatkan secara gratis sehingga bisa memberikan keuntungan ekonomis dengan menekan anggaran untuk membeli lisensi software.

Sistem operasi open source seperti Linux menawarkan berbagai distribusi (distro) seperti Ubuntu, RedHat, Fedora dan lainnya. Ubuntu sendiri menjadi sistem operasi open source yang paling populer saat ini. Hal yang harus diperhatikan dalam mulai menggunakan sistem operasi berbasis open source adalah adaptasi dari pihak user dikarenakan sistem operasi open source memiliki sedikit perbedaan dibandingkan dengan sistem operasi Windows.

Sumber referensi:

-Aneka ragam serangan di dunia maya – ID-SIRTII

http://berkomputer.com/info/apa-itu-malware-dan-perbedaan-jenis-jenis-malware/

http://freesharefor.us/archive/index.php/thread-185.html

Bogor, 6 Februari 2011

Minggu 12:41

Mochammad Firdaus Agung / mfirdausagung@gmail.com

Teknik Informatika Universitas Diponegoro / www.if.undip.ac.id

Saat ini sedang melakukan praktek kerja lapangan di ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) / www.idsirtii.or.id