Oleh Diyanah Anuar
diyanah@bharian.com.my

BH, 27 Jun 09
P-16

virus komputer

Tip elak sistem komputer lumpuh

GANGGUAN teknikal pada sistem komputer sebolehnya dielak kerana hanya melambatkan proses kerja. Paling bengang, setiap kali ada tugasan penting hendak diselesaikan, detik itu jugalah komputer meragam.

Salah satu penyebab masalah teknikal pada sistem komputer ialah isu serangan virus. Masalah ini sering berpunca daripada tindakan pengguna sendiri hingga komputer dihinggapi virus yang merebak dan merosakkan bahagian tertentu.

Virus berbahaya kepada komputer kerana dengan pantas boleh memenuhi memori peralatan ini. Virus kemudian melumpuh atau menjadikan sistem komputer tidak lagi berfungsi. Lebih serius lagi, ia boleh disebarkan melalui jaringan (network) dan menembusi sistem keselamatan komputer.

Jika diperhatikan, ramai pengguna kurang prihatin dalam melengkapkan komputer dengan sistem perlindungan virus serta ancaman lain terhadap sistem komputer.

Ramai juga hanya menggunakan program keselamatan dan antivirus yang dimuat turun secara online. Program ini lazimnya cuma boleh digunakan dalam tempoh tertentu serta agak lemah dalam mengekang kehadiran virus terutama virus baru. Kesannya, komputer terdedah dengan serangan virus dan ancaman lain.

Kolum Tanya Pakar merujuk Ketua Perniagaan Norton

"Muat turun secara percuma juga boleh berdepan dengan risiko malware, komitmen langganan yang berterusan atau anda akan tersenarai dalam penerima e-mel spam"

Effendy Ibrahim
Ketua Perniagaan Norton Asia Selatan

anda melawat sesebuah laman dan mengaktifkan program yang sedia ada di situ.

Dalam pautan (attachment) e-mel pula, pencipta virus suka menghantar e-mel kepada banyak alamat pada satu masa serta cuba menarik perhatian penerima e-mel untuk mengaktifkan virus yang sudah mereka sembunyi dalam fail pautan yang dihantar dalam e-mel itu. Kaedah yang sama juga dilakukan dengan pautan fail pada mesej segera atau

Asia Selatan, Effendy Ibrahim, mengenai kepentingan sistem perlindungan keselamatan komputer. Beliau yang bertanggungjawab dalam merancang, memasar serta merangka program pendidikan pelanggan juga berkongsi tip mengelak serangan virus pada sistem komputer.

Mengapa pengguna perlu mengambil berat soal virus komputer?

Menurut laporan terbaru Symantec mengenai ancaman keselamatan internet, jumlah dan penyebaran kod program yang merosakkan (malicious code) meningkat dengan pantasnya tahun lalu.

Ini menyebabkan Symantec perlu mencipta lebih daripada 1.6 juta malicious code signature yang baru untuk membantu menghalang 245 juta cubaan serangan malicious code di seluruh dunia pada setiap bulan, sepanjang tahun lalu.

Ancaman terhadap komputer menjadi semakin rumit malah bentuk ancaman berkembang lebih daripada sekadar virus. Ancaman dari aktiviti online yang makin berkembang juga sedikit sebanyak mengubah konsep perlindungan komputer untuk bertindak terhadap ancaman seperti trojan horses, worms dan spyware yang sering datang dari laman web yang dilayari. Ini secara tidak langsung meletakkan pengguna dalam risiko ruang siber.

Lihat saja berapa banyak aktiviti online yang kita lakukan hari-hari, sama ada menghantar atau menerima e-mel; berkongsi foto dan fail; bersembang; bermain permainan online; muat turun muzik; video dan sebagainya.

Malangnya, apa saja yang kita simpan dalam komputer berdepan dengan risiko setiap kali kita online termasuk identiti, kata laluan dan maklumat peribadi kita.

Virus komputer hanya sebahagian kecil daripada ancaman komputer. Biasanya, ia dimuat turun secara tidak sengaja dan akan 'tinggal' dalam sebuah fail. Apabila anda membuka fail itu, virus menjadi aktif.

Ini boleh memberi kesan serius. Antaranya, merosakkan sistem komputer, mencuri maklumat identiti anda, menjangkiti fail yang anda hantar kepada orang lain selain tersebar sendiri kepada sesiapa yang berada dalam buku alamat e-mel anda.

Apakah jenis virus yang biasa menyerang komputer? Fail yang bagaimana boleh dijangkiti virus?

Ada lima virus komputer yang terkenal.

1. Virus file infector

Virus ini menyerang fail program dan lazimnya menyerang kod seperti .com dan fail .exe. Ia boleh menyerang fail lain apabila sesebuah program yang sudah dijangkiti dipasang dari floppy, hard drive atau jaringan (network).

2. Virus boot sector

Menyerang bahagian sistem dalam sebuah disk iaitu rekod boot dalam floppy disk dan hard disk. Semua floppy disk dan hard disk mempunyai program kecil dalam rekod boot yang akan berjalan sebaik komputer mula dihidupkan. Virus Boot Sector menjangkiti bahagian dalam disk ini dan aktifkan apabila anda menggunakan disk yang sudah dijangkiti.

3. Virus master boot sector

Virus jenis menetap di memori ini menyerang disk dengan cara yang sama seperti virus boot sector. Beza antara kedua-dua virus ini adalah di mana kod virusnya terletak. Rekod master boot biasanya menyimpan salinan rekod master boot di lokasi berlainan. Komputer Windows NT yang dijangkiti virus ini tidak akan boot (hidup semula)

4. Virus Multipartite

Menyerang kedua-dua rekod boot dan fail program dan sukar untuk dibaiki. Jika bahagian boot bersih, tapi fail tidak bersih, bahagian boot boleh dijangkiti semula.

5. Virus Mikro

Virus jenis ini akan menyerang fail data. Virus ini adalah yang paling biasa menyerang dan mempunyai kos paling tinggi untuk memperbaikinya.

Bagaimana virus disebarkan?

Ketika anda melayari internet, ada banyak cara untuk anda terjebak dengan serangan virus yang merosakkan. Senario yang lazim berlaku, pencipta virus akan mengeksploitasi browser anda yang terdedah kemudian memuat turun malicious code pada bahagian latar belakang, ketika anda melawat sesebuah laman.

Ada juga yang menggunakan skrip program yang kecil untuk menyerang komputer ketika instant messenger (IM).

Penggodam masa kini menggunakan pelbagai muslihat untuk 'memujuk' anda membuka dokumen Word yang mempunyai virus, antaranya dengan menampakkan seolah-olah ada mesej penting untuk anda dalam dokumen berkenaan.

Contohnya, ketika perhatian tertumpu kepada penularan wabak H1N1 sekarang ini, ramai penggodam menyebarkan emel yang mempunyai pautan Adobe yang bertajuk Swine influenza frequently asked questions.pdf.. Apabila pengguna membuka fail berkenaan, malcode di dalam pdf akan cuba meninggalkan malware dalam sistem komputer pengguna itu.

Satu lagi ancaman atau jenayah siber yang membimbangkan adalah phishing. Penjenayah siber ini menggunakan spam, laman web palsu, crimeware dan teknik lain untuk mengelirukan orang lain hingga mereka memberi maklumat peribadi yang sepatutnya dirahsiakan. Apabila memperoleh maklumat itu, mereka akan menggunakannya untuk mencuri atau menjual maklumat pengguna itu kepada pasaran gelap yang dipanggil *underground economy*.

LIHAT MUKA 21