

# Yoga Prihastomo

*Keamanan Sistem Komputer*

2003-31-038

1. *Malicious Code* merupakan kode program yang ditulis untuk tujuan yang dapat merugikan keamanan sistem komputer. Malicious code dikategorikan berbahaya karena dapat mencuri data korban dan dikirimkan ke sang pembuat. Dan bahkan dapat melakukan modifikasi dan informasi yang dikategorikan rahasia / konfidensial, serta melakukan perubahan pada konfigurasi dan komputer.
2. Jenis-Jenis Malicious Code :
  - *Virus* merujuk pada program yang memiliki kemampuan untuk her- reproduksi, menulari program lain dan menjadikan file-file program tertular sebagai file infector.
  - *Worm* merupakan program yang dibuat dimana penyebarannya dengan mengcopy dirinya sendiri dari satu sistem ke sistem yang lain biasanya melalui jaringan komputer.
  - *Adware* merupakan program yang akan menampilkan iklan *pop-up* (muncul dalam layar tersendiri) pada saat program tersebut di jalankan. (umumnya program ini tersedia di Internet secara gratis dari iklan yang ditampilkan tersebut menambah income bagi perusahaan.
  - *Spyware* biasanya didapatkan pada saat melakukan browsing ke situs tertentu dan aplikasi ini terinstall biasanya tanpa sepengetahuan kita. Spyware juga dapat menyebabkan koneksi ke Internet menjadi lambat, mengurangi kinerja dan komputer tersebut, dan yang paling parah adalah hilangnya (dicurinya) informasi yang bersifat pribadi.
  - *Trojan Horse* merujuk pada program independen yang tampaknya berguna, dan ketika dieksekusi, tanpa sepengetahuan pengguna, juga melaksanakan fungsi-fungsi yang bersifat destruktif dan merugikan. Program ini sangat berbahaya karena bisa dijadikan sebagai pintu masuk ke sistem yang terinfeksi.
  - *Malware* merupakan singkatan dari *malicious software*, merujuk pada program yang dibuat dengan tujuan membahayakan atau menyerang sebuah sistem komputer.
  - *Malicious toolkits* merujuk pada program yang didesain untuk membantu menciptakan program-program yang dapat membahayakan sebuah sistem komputer. Contoh dari program jenis ini adalah tool pembuat virus dan program yang dibuat untuk membantu proses hacking.
  - *Joke program* merujuk pada program yang meniru operasi-operasi yang dapat membahayakan sistem komputer, namun sebenarnya dibuat untuk tujuan lelucon dan tidak mengandung operasi berbahaya apapun.

- *Spam* merupakan code program yang biasanya ditujukan pada email seseorang. Program / code ini bersifat tidak berguna bahkan ada yang cenderung membahayakan. Spam ini biasanya berupa iklan terselubung.
  - *Riskware* berupa program atau code program yang ditujukan untuk membahayakan sistem keamanan komputer.
  - *Key Logger* merupakan program yang fungsinya untuk memata-matai aktifitas user. Fungsinya hampir sama dengan spyware.
- a. Perilaku & Resiko yang ditimbulkan !
- ✓ Worm & virus dapat merusak dan menggandakan diri pada sistem yang terinfeksi
  - ✓ Adware mengganggu kita dikala browsing, sering kali adware disusupi oleh virus.
  - ✓ Spyware dapat memata-matai komputer korban, sering kali membuat back door pada komputer yang terinfeksi.
  - ✓ Trojan horse dapat mengambil alih komputer korban tanpa sepengetahuan (secara tersembunyi)
  - ✓ Malicious Tools kit menganalisa celah keamanan pada komputer targer (korban) sehingga memudahkan hacker untuk menguasai komputer korban.
  - ✓ Joke program hanya bersifat lelucon, biasanya tidak berbahaya, namun untuk kasus tertentu dapat mengganggu.
  - ✓ Spam berisi iklan yang tidak jelas, menggunakan teknik DoS (*Denial of Service*) yang dampaknya dapat membuat inbox email menjadi penuh.
  - ✓ Key Logger dapat melakukan logging / mencatat aktivitas user. Jadi dapat memata-matai si pengguna komputer.

Secara keseluruhan, Malicious code dapat merugikan atau membahayakan keamanan sistem komputer kita. Baik disadari ataupun tidak, sistem yang disusupi malicious code dapat mengalami penurunan kinerja.

- b. Resources yang diserang & yang dilakukan terhadap komponen tersebut !
- Malicious code dapat menyerang :
- ✓ Software seperti : Sistem Operasi, Aplikasi (beberapa virus menyerang file .exe sehingga tidak dapat dieksekusi).
  - ✓ Hardware, beberapa virus diketahui dapat menyebabkan kerusakan pada hardware.
  - ✓ Beberapa virus dapat menyebabkan hilangnya data pada komputer kita.
  - ✓ Virus dan variannya secara cerdas dapat menyerang program AntiVirus dan sejenisnya.

Yang dilakukan terhadap resources :

- ✓ Malicious secara umum dapat merugikan keamanan komputer kita.
- ✓ Pada software dapat melakukan penyerangan yang mengakibatkan komputer dapat diambil alih oleh hacker.
- ✓ Membuat resources terpakai secara berlebihan tanpa terkendali (DoS).

- c. Tindakan pencegahan
    - ✓ Pasang Anti Virus, Anti Sypware, Anti Adware dan program lain sejenisnya pada sistem kita.
    - ✓ Update database program anti virus secara teratur
    - ✓ Pergunakan Firewall Personal, dengan menggunakan firewall maka akses yang akan keluar-masuk ke system kita dapat diatur, apakah paket data disetujui atau ditolak.
    - ✓ Berhati-hati sebelum menjalankan file baru
    - ✓ Buat Policy / Kebijakan keamanan yang jelas
  - d. Tindakan deteksi yang dapat diterapkan
    - ✓ Gunakan software Anti Virus, Anti Sypware, Anti Adware dan program lain sejenisnya pada sistem kita.
    - ✓ Gunakan Firewall, IDS (Intrusion Detection System), IPS (Intrusion Prevention System) pada komputer dan jaringan komputer kita.
  - e. Perbaikan yang dapat dilakukan
    - ✓ Hilangkan macilious code dengan Security Tools.
    - ✓ Repair menggunakan utility bawaan dari Security Tools.
    - ✓ Untuk data yang hilang, gunakan program recovery data seperti Get Data Back, Easy Recovery, dll.
    - ✓ Disarankan untuk membackup data sebulan sekali.
3. Tindakan penyerangan terhadap jaringan komputer
- Penyerangan yang bersifat fisik, seperti melakukan sabotase pada jaringan komputer. Termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
  - *Wiretapping* atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
  - *Denial of Service*, yaitu akibat yang ditimbulkan sehingga servis tidak dapat diterima oleh pemakai juga dapat dimasukkan ke dalam kelas ini.
  - "*Social Engineering*" yang sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi.
  - *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
  - *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.
- a. Perilaku & Resiko yang ditimbulkan !
- ✓ Semua teknik di atas dilakukan atas dasar adanya lubang keamanan pada sistem setelah mereka menganalisa keamanan pada jaringan komputer.

- ✓ Teknik di atas memungkinkan seseorang untuk membuat back door, memata-matai jaringan, menghabiskan resources bahkan sampai mengambil alih jaringan secara logical.
  - ✓ Teknik penyerangan secara fisik, dapat menyebabkan kerusakan pada jaringan komputer secara langsung.
  - ✓ Social Engineering, biasanya menjadi sesuatu yang tidak disadari administrator jaringan
- b. Resources yang diserang & yang dilakukan terhadap komponen tersebut !  
Resources yang diserang dapat berupa software (sistem operasi dan aplikasi), jaringan secara fisik (router, firewall, kabel, dsb).
- c. Tindakan pencegahan
- ✓ Gunakan software Anti Virus, Anti Spyware, Anti Adware dan program lain sejenisnya pada sistem kita.
  - ✓ Kombinasikan firewall, IDS dan IPS secara optimal baik secara software maupun secara hardware.
  - ✓ Gunakan proxy server untuk menjaga jaringan kita.
  - ✓ Gunakan tools tambahan untuk menyembunyikan sistem kita dari internet.
- d. Tindakan deteksi yang dapat diterapkan
- ✓ Gunakan Firewall, IDS (Intrusion Detection System), IPS (Intrusion Prevention System) pada komputer dan jaringan komputer kita.
  - ✓ Gunakan Tools untuk memantau aktivitas jaringan kita.
  - ✓ Terapkan security policy yang baik pada jaringan.
  - ✓ Kenalilah “musuh dalam selimut” yang ada pada sistem kita.
- e. Perbaikan yang dapat dilakukan.
- ✓ Perbaiki pemasangan kabel pada jaringan.
  - ✓ Untuk beberapa kondisi, batasi lalu-lintas kabel, dengan kata lain tanamlah kabel pada dinding atau gunakan pelindung.
  - ✓ Firewall, IDS dan IPS harus selalu di update.