STUDI SISTEM KEAMANAN KOMPUTER

Tri Wahyu W, Aidil Sanjaya
Jurusan Teknik Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
Jl. Raya Sawo Manila, Pejaten No. 61, Jakarta 12520

ABSTRACT

On this paper we investigate the security system in computer through literature on the web. Security system has an important role in keeping the secrecy of personal data. Indeed if the computer is connecting to internet. Privacy is serious problem when we don't take serious care on security systems. Mal-ware and spamm email are one of the problem that need to be handled in order keeping those.

Keywords: security systems, mal-ware, spamm

ABSTRAK

Keamanan komputer yang dianggap tidak penting oleh banyak orang ternyata dapat membawa kerugian besar bagi orang tersebut. Jika ditelaah lebih lanjut ternyata banyak hal – hal yang dapat mengancam data – data pribadi seseorang melalui media komputer. Saat ini sudah banyak program – program yang bersifat jahat seperti virus, worm, trojan dan lainnya yang bila menginfeksi sistem komputer kita dapat mengakibatkan kerugian bagi kita. Penelitian itupun tidak hanya berdasarkan pengalaman pribadi, tetapi juga dirangkum dari berbagai sumber pustaka yang didapat dari internet dimana dengan media internet kita bisa mengetahui kejahatan apa saja yang telah terjadi yang disebabkan oleh malicious software tersebut. Adapun cara untuk mengamankan komputer kita dari serangan malicious software, yaitu dengan menggunakan program yang disebut anti-virus. Dengan program anti-virus ini kita setidaknya dapat mencegah masuknya *malicious software* dalam komputer kita, walaupun mungkin kita tidak merasa nyaman dengan penggunaan anti-virus tersebut. Seperti kata banyak orang, jika ingin aman maka tidak akan nyaman.

Kata kunci: Sistem keamanan komputer, *mal-ware, spamm*

I. PENDAHULUAN

Seperti yang kita ketahui, saat ini hampir semua pekerjaan membutuhkan komputer, dan hampir semuanya menyimpan data – data pekerjaan tersebut dalam komputer. Data – data yang disimpan dalam komputer itu bisa berupa data *public* maupun data penting suatu perusahaan. Data – data penting suatu perusahaan seharusnya tidak dapat diakses oleh orang lain diluar perusahaan tersebut. Tetapi pada masa sekarang, banyak sekali perusahaan yang tidak memperdulikan mengenai keamanan di komputer mereka, dan akhirnya menyebabkan ada pihak dari luar perusahaan yang dapat mengakses serta mengambil atau mengubah data – data penting perusahaan tersebut.

Maka dari itu, keamanan komputer sangat perlu untuk digunakan, tidak hanya oleh perusahaan besar saja, melainkan oleh semua orang yang menggunakan komputer. Jika kita tidak ingin ada orang lain yang dapat mengakses data kita, maka kita harus memperhatikan keamanan

dalam komputer kita. Ada beberapa cara yang dapat digunakan oleh pihak lain untuk mengakses komputer kita, tetapi ada juga beberapa cara bagi kita untuk mengamankan komputer kita tersebut.

Ada *program* yang disebut sebagai *Malicious Software*, atau yang bisa disingkat menjadi *Malware*, yaitu suatu *software* yang di-*design* untuk merusak sistem komputer tanpa memberitahu pemilik komputer tersebut. *Malware* sendiri dapat dibagi menjadi beberapa jenis, diantaranya adalah *computer virus*, *worm*, *trojan*, dan masih banyak yang lain.

Ada juga *program* yang dapat mencegah *Malicious Software*, seperti *anti-virus, firewall,* dan *program – program* sejenisnya. Dengan *program* ini kita dapat mengetahui apabila ada *malware* yang masuk ke dalam komputer kita, dan kita dapat mencegah atau menghapus *malware* tersebut.

Metode yang kami gunakan dalam melakukan analisis terhadap masalah ini adalah dengan menggunakan metodologi kepustakaan, dimana data – data yang kami perlukan didapatkan dari berbagai sumber pustaka melalui internet.

II. DASAR TEORI: PENGERTIAN *COMPUTER SECURITY*

Computer Security adalah bagian dari ilmu komputer yang bertugas untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. *Computer Security* yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (*Internet*), dari akses yang tidak memiliki hak untuk mencoba masuk untuk memperoleh informasi dan *service* tertentu yang ada di dalam sistem. Usaha untuk mengakses paksa ini terdapat banyak macamnya, baik itu *intrusion* (serangan dari luar organisasi) atau *misuse* (serangan dari dalam organisasi), dengan *level hacker* (hanya mencoba masuk ke dalam sistem komputer) atau bahkan *cracker* (mencoba masuk dan merusak untuk keuntungan pribadi).

2.1 Pengertian *Malicious Software*

Seperti yang sudah dijelaskan di Latar Belakang, *Malicious Software* atau *Malware* merupakan suatu program yang dapat merusak sistem komputer kita tanpa kita sadari. *Malware* sendiri terdiri dari beberapa kelompok, yaitu :

a. *Infectious Malware*, yaitu *malware* yang meng-infeksi sistem dalam komputer kita. Jenis dalam tipe *malware* ini adalah *computer viruses* dan *computer worms*. Sering kali kita berpikir bahwa *computer viruses* dan *worms* adalah sama, padahal sebenarnya tidak jika dilihat dari bagaimana cara penyebarannya. Berikut akan dibahas mengenai tipe – tipe dari *infectious malware*.
   - Sebelum *internet access* digunakan secara luas, penyebaran *virus* pada PC adalah dengan menginfeksi *programs* atau *executable boot sectors* pada *floppy disks*. *Computer virus* akan menginfeksi *executable software* dan akan menginfeksi sistem komputer kita bila kita menjalankan *executable software* yang sudah terinfeksi oleh *virus* tersebut.
   - *Worms* pertama kali dibuat bukan dalam komputer biasa, tetapi dalam sistem Unix. *Worms* yang pertama kali dikenal adalah *Internet Worm* (1988), yang menginfeksi SunOS dan sistem VAX BSD. Tidak seperti *virus*, *worms* tidak memasukkan dirinya ke dalam program lain. Melainkan dengan cara mengexploitasi lubang *security* pada *network server programs* dan mulai menjalankan dirinya sebagai proses yang berbeda. Saat ini *worms* sering dibuat untuk *Windows OS*, walaupun dibuat juga untuk sistem *Linux* dan *Unix*. Cara kerja *worms* memiliki *basic* yang sama dengan *Internet Worm* pada tahun 1988, yaitu dengan men-*scan* komputer dalam jaringan yang dapat diakses, kemudian meng-*copy* dirinya sendiri.

b. *Concealment Malware*, yaitu *malware* yang secara diam – diam masuk dalam komputer kita. *Malware* tipe ini dapat bekerja dalam komputer kita tanpa diketahui oleh pengguna komputer tersebut. Cara kerja *malware* tipe ini mirip dengan teknik *Trojan horse* atau *trojan*. *Trojan horse* adalah *program* yang meminta pengguna untuk menjalankannya, namun secara diam – diam memasukkan *tools* yang berbahaya. *Tools* tersebut dapat menyebabkan efek langsung, dan efek-

nya pun dapat bermacam – macam, seperti menghapus semua file pengguna, atau lebih umum lagi dapat meng-*install software* berbahaya ke dalam sistem pengguna untuk tujuan jangka panjang. Satu dari banyak cara *spyware* termasuk dalam *Trojan horse*, adalah dengan menyatukan *Trojan program* tersebut dalam sebuah *software* yang di-*download* oleh pengguna melalui *Web* atau *file – sharing*. Ketika pengguna meng-*install software* yang di-*download* tersebut, secara otomatis *spyware* juga ter-*install*. Sekali *malicious program* ter-*install* dalam sistem, itu memungkinkan pembuat *malicious program* tersebut tersembunyi, sama saja ketika seseorang menyerang langsung ke komputer tersebut.

Teknik tersebut dikenal sebagai *rootkits* yang memperbolehkan persembunyian ini dengan cara mengubah sistem operasi komputer sehingga *malware* tersebut disembunyikan dari pengguna. *Rootkits* dapat mencegah laporan sebuah proses *malicious* dalam tabel proses atau menjaga *file* tersebut dari status *read*.

c. *Malware for profit*, yaitu *malware* yang digunakan untuk mencari keuntungan. Ada beberapa *malware* pada tipe ini, diantaranya adalah *spyware, botnets, loggers,* dan *dialers*.

- *Spyware* adalah produksi yang memungkinkan pengumpulan informasi mengenai komputer pengguna, memperlihatkan iklan, atau menggunakan kebiasaan *web-browser* untuk keuntungan finansial bagi pembuat *spyware* tersebut. Biasanya, beberapa *spyware programs* mengubah hasil *search engine* menjadi iklan. *Spyware* biasanya ter-*install* sebagai *trojan horses*.
- *Spammer viruses*, seperti kelompok virus Sobig dan Mydoom, mendapatkan komisi dari *e-mail spam*. Komputer yang terinfeksi digunakan sebagai *proxies* untuk mengirimkan pesan yang bertipe *spam*. Keuntungan *spammers* menggunakan komputer yang terinfeksi adalah kemungkinan penyebaran dalam jumlah besar dan sumbernya tidak diketahui, dan juga mengamankan *spammer* dari tuntutan. *Spammers* juga menggunakan komputer yang terinfeksi untuk menyerang organisasi *anti-spam* dengan *Distributted Denial-of-*Service *(D-DoS) attack.*
- *Botnets*. Dalam *botnets*, *malware* masuk ke dalam sebuah *Internet Relay Chat (IRC) channel*, atau sistem *chat* lainnya. Penyerang dapat memberikan instruksi pada semua sistem yang terinfeksi secara simultan.
- Mungkin untuk pembuat *malware* mencari keuntungan dengan mencuri informasi dari seseorang yang komputer-nya terinfeksi. Beberapa *malware programs* meng-*install* sebuah *keylogger*, dimana meng-*copy* semua ketikan pengguna pada keyboard ketika mengetik *password,* nomor *credit card*, atau informasi lainnya yang mungkin berguna bagi pembuat *malware*. Kemudian data ini dikirim secara otomatis ke pembuat *malware* tersebut, memperbolehkan penipuan *credit card* dan kejahatan pencurian lainnya. *Keylogger* juga dapat meng-*copy CD-Key* atau *password* pada *online games*, yang memungkinkan pembuat untuk mencuri *accounts* atau *virtual items*.
- Cara lainnya untuk mencuri uang dari komputer yang terinfeksi adalah dengan mengontrol *modem* dan men-*dial* nomor telepon yang mahal. *Dialer* atau *Porn Dialer software* men-*dial* sebuah nomor telepon premium yang mahal dan meninggalkan *dial* tersebut sehingga korban harus membayar biaya telepon itu.

III.ANALISA PENYEBAB KOMPUTER TERKENA SERANGAN *MALWARE*

Ada beberapa penyebab kenapa komputer bisa terkena serangan *malware*. Yang paling penting adalah dari segi keamanan pada komputer kita. Berikut akan dibahas penyebab – penyebab kenapa komputer bisa terkena serangan *malware*.

- Kelengahan dari pengguna.

Penyebab paling utama dan paling sering terjadi adalah karena kelengahan atau kesalahan dari pengguna komputer tersebut. Hal yang paling dasar adalah pada saat kita men-*download* suatu *file*, jika *file* tersebut mengandung *malware*, tanpa kita sadari kita memasukkan *malware* tersebut ke dalam komputer kita. Kemudian ada juga kesalahan ketika kita membuka *file* dari *storage disk*

seperti *floppy disk* atau *flashdisk* dan semacamnya, bisa saja *storage disk* tersebut sudah terinfeksi oleh *malware* dan *malware* tersebut sudah menginfeksi *file* yang ada di dalam *storage disk* tersebut dan kita membuka *file* tersebut, secara otomatis komputer yang kita gunakan sudah mengakses *malware* yang ada dalam *file* tersebut.

- Komputer belum mempunyai sistem keamanan yang baik.

Penyebab lainnya yang juga sering terjadi yaitu berasal dari sistem yang ada di komputer kita. Sering kali kita lengah dan merasa keamanan komputer itu tidaklah penting. Keamanan komputer memang tidak perlu diperhatikan jika pada komputer kita tidak ada perangkat lain seperti *floppy disk, cd/dvd-rom, usb, internet,* dan juga tidak terhubung dalam jaringan. Jadi komputer kita hanya digunakan untuk keperluan dalam komputer itu saja, dan *file* dari luar komputer tidak bisa masuk ke dalam komputer, dan *file* dalam komputer juga tidak bisa di-*copy* keluar. Tetapi jika komputer kita mempunyai salah satu saja dari perangkat diatas, maka keamanan pada komputer harus sangat kita perhatikan. Mengapa kita harus memperhatikan keamanan komputer? Saat ini sudah banyak *malware* yang dapat merusak sistem komputer kita. Bayangkan ketika ada data penting anda hilang atau diambil oleh orang lain tanpa seijin anda. Bayangkan ketika data pribadi perusahaan anda diambil oleh saingan perusahaan anda. Banyak sekali kerugian yang didapatkan hanya karena komputer belum mempunyai sistem keamanan yang baik.

- *Hole – hole* dalam sistem operasi yang dipakai.

Penyebab lain yang tidak berhubungan langsung dengan pengguna adalah lubang – lubang *security* yang terdapat pada sistem operasi yang kita pakai. Banyak pelaku kejahatan cyber menggunakan lubang – lubang *security* tersebut karena sifatnya sama di tiap komputer, apalagi bila sistem operasi pada komputer – komputer tersebut belum di-*update*. Bagaimana cara meng-*update* / menutup lubang – lubang *security* pada komputer kita? Caranya ialah kita harus meng-*update* melalui website dari sistem operasi yang kita gunakan. Misalnya saja kita menggunakan sistem operasi berbasis Windows. Untuk meng-*update*-nya maka kita harus masuk ke situs Microsoft, dan men-*download file update* tersebut, atau yang banyak disebut sebagai *hotfix*. Masalahnya, saat ini untuk dapat meng-*update* sistem operasi tersebut, sistem operasi yang kita gunakan harus di-*detect* sebagai sistem operasi yang asli (bukan bajakan). Padahal sedikit sekali dari kita yang menggunakan sistem operasi yang asli karena harganya yang bisa dikatakan mahal. Jadi *update* dari sistem operasi ini sering kali dilupakan oleh pengguna komputer padahal celah – celah inilah yang paling sering digunakan para *hacker* untuk menembus sistem keamanan di komputer kita.

- Penyebab lainnya

Penyebab lain yang mungkin tidak berhubungan sama sekali dengan pengguna / korban adalah bila korban menggunakan komputer di tempat umum seperti warnet. Bisa saja komputer tersebut menggunakan *malware keylogger*. Korban tanpa sadar memasukkan data – data rahasia seperti *password*, *PIN*, maupun data lainnya yang sangat penting. Lalu si pelaku bisa melihat apa saja data penting korban tersebut dan menggunakannya tanpa ijin dan membuat kerugian besar terhadap korban.

Contoh Kasus

Ada beberapa contoh kasus dalam penggunaan *program malware* ini. Berikut adalah contoh – contoh kasus yang pernah terjadi :

a. Penyebaran *Virus Brontok*.

Beberapa saat lalu, dunia komputer dikejutkan oleh adanya *virus* yang dinamakan *Brontok* / *RontokBro*. Cara kerja *virus* ini adalah dengan menginfeksikan dirinya ke dalam suatu *file*, dan akan menginfeksi sistem komputer apabila kita membuka *file* yang terinfeksi tersebut. Sebab – sebab yang diakibatkan oleh *virus* ini yaitu hilangnya sistem regedit dari komputer kita, kemudian kita tidak bisa membuka '*Folder Option'* yang harusnya tersedia pada '*Control Panel'*.

Ketika pertama kali muncul, tidak banyak orang yang tahu bagaimana cara menghilangkan *virus* ini karena *anti-virus* yang ada belum memiliki cara untuk menghapus dan membersihkan komputer dari *virus* ini. Pada waktu itu, cara yang paling sering digunakan oleh banyak orang adalah dengan mem-*format* komputer agar sistem dapat kembali seperti baru. Tapi bila *file* yang berisikan *virus brontok* ini masuk ada di komputer kita, dan kita membuka kembali *file* tersebut, ya secara otomatis *virus* itu akan menginfeksi sistem komputer kita lagi. Sampai saat ini *virus brontok* masih tersebar di berbagai komputer terutama komputer yang tidak memiliki keamanan dan komputer pada warnet – warnet.

b. Penyebaran *Worm Blaster*.
Beberapa tahun yang lalu, para pengguna komputer mungkin terkejut ketika sedang menggunakan komputer kemudian ada pemberitahuan bahwa komputer akan *restart* dalam waktu 60 detik, dan ada *timer countdown* pada pesan tersebut. Kita tidak dapat menutup pesan tersebut karena pesan tersebut. Kemudian setelah 60 detik maka komputer kita akan *restart* dengan sendirinya, dan kemudian beberapa saat setelah *restart*, pesan tersebut kembali muncul, dan hal itu terjadi berulang – ulang tanpa sempat kita mencari dimana kesalahannya. Setelah beberapa hari kemudian ada *update* dari produsen *anti-virus* agar *worm blaster* tersebut dapat dihapus dengan menggunakan *anti-virus* tersebut. Tetapi bagaimana kita bisa menghapus *worm* tersebut sedangkan setiap beberapa menit komputer kita *restart* dengan sendirinya? Hal ini bisa diakali dengan menggunakan cara '*Safe Mode Logon'* yang ada pada setiap sistem operasi. Dengan menggunakan fasilitas *Safe Mode*, maka kita bisa men-*scan* komputer kita dan menghapus *worm* tersebut. Pada saat ini *worm blaster* sudah jarang ditemui pada komputer – komputer apabila komputer tersebut sudah memiliki sistem keamanan yang bisa dibilang lumayan baru, karena *update* untuk *worm blaster* ini sudah lama dikeluarkan oleh *vendor – vendor anti-virus* yang ada.

c. Penggunaan *Credit Card* orang lain.
Kasus yang ini paling susah untuk dideteksi apabila komputer kita tidak memiliki sistem keamanan yang baik. Pada kasus ini *tools malware* yang paling sering digunakan adalah *keylogger*. Dengan menggunakan *keylogger* maka apa yang kita ketik pada keyboard akan tercatat pada suatu *file log* dan *file* tersebut dapat dikirim secara otomatis kepada pelaku. Pelaku kemudian melihat manakah data – data penting yang bisa diambil, misalnya nomor kartu kredit beserta *password* atau *PIN* untuk menggunakan kartu tersebut. Kemudian secara bebas pelaku menggunakan kartu kredit korban untuk mencari keuntungan lainnya. Yang membuat *tools* ini sulit dideteksi disebabkan karena ada beberapa *tools keylogger* yang tidak terdeteksi oleh *anti-virus* yang terbaru sekalipun.

d. *Spamming*.
Cara kerja *spamming* adalah dengan mengirim *e-mail* iklan dan sebagainya secara otomatis dan akan hal ini akan dilakukan secara terus menerus tanpa bisa dihentikan kecuali *mail server* yang kita gunakan dapat membedakan mana *e-mail* yang bersifat *spam* dan mana *e-mail* yang bukan *spam*. *Spamming* sebenarnya tidak terkait langsung dengan masalah keamanan komputer, tetapi berkaitan oleh pengguna. Sering kita masuk ke suatu situs dan kemudian situs tersebut meminta alamat email kita. Alamat email yang kita isi kemudian akan dikirimi *e-mail* yang bila kita buka maka dengan otomatis *malware* tersebut terinstall secara diam – diam di komputer kita, dan akan mengirimkan *e-mail – e-mail* pada semua alamat *e-mail* yang ada pada *address book* kita, dan hal ini dilakukan terus menerus, dan akan dilanjutkan apabila ada orang lain yang membuka *e-mail* tersebut. *Program spamming* ini adalah salah satu *malware* yang paling sulit untuk dihilangkan. Karena dengan menggunakan *software* tertentu, setiap orang bisa membuat *program* yang mirip dengan *program spamming*.

e. *Spyware, Trojan horse, Adware*.
Contoh lain adalah kasus *malware* yang berhubungan dengan *Spyware, Trojan horse*, dan *Adware*. Cara kerja *Spyware* sebenarnya mirip dengan *Trojan horse*, yaitu menginfeksi sistem komputer kita secara sembunyi – sembunyi dan biasanya ikut ter-*install* ketika kita meng-*install program* lain. Kasus yang berhubungan dengan *Trojan* dan *Spyware* yaitu ketika ada orang lain

yang dapat mengakses data dalam komputer kita, mengubahnya, serta menghapus data tersebut. Untuk kasus *Adware*, banyak terjadi di warnet – warnet umum yang tidak memiliki sistem keamanan yang baik. Pada komputer di warnet tersebut, ketika kita membuka 1 halaman *Internet Explorer*, maka secara otomatis akan muncul *Pop-Up – Pop-Up* yang berisi iklan – iklan, dan kebanyakan merupakan iklan porno. Jika kita mengklik iklan tersebut, bisa saja ada *malware* lainnya yang menginfeksi sistem komputer kita. *Adware* biasanya menginfeksi komputer yang penggunanya suka mengakses situs – situs porno, dan situs – situs yang menyediakan *crack* untuk *program – program* yang sebenarnya harus dibeli. Selain itu *adware* juga dapat menyebar seperti *spyware* dan *trojan*, yaitu dengan ikut serta dalam suatu *program*. Sampai saat ini penggunaan *Spyware, Trojan horse,* dan *Adware* juga susah dihilangkan karena ini tergantung dengan pengguna, apabila pengguna sering meng-*install program* tanpa melihat – lihat '*Terms and Agreement*'-nya, karena biasanya pemberitahuan mengenai *Spyware* dan *Trojan* ada pada '*Terms and Agreement*' yang ada pada saat kita meng-*install* suatu *program*.

IV. PEMBAHASAN

Diatas kita sudah membahas mengenai permasalahan – permasalahan yang berkaitan dengan *computer security* beserta contoh – contoh kasus yang sudah terjadi. Sekarang kita akan membahas mengenai bagaimana cara kita menangani / menyelesaikan permasalahan tersebut.

Seperti yang sudah disebutkan diatas, penyebab komputer kita terinfeksi oleh *malware* adalah karena kelengahan pengguna, sistem keamanan komputer kita, serta *hole – hole* dalam sistem operasi yang digunakan. Cara menghilangkan penyebab yang dikarenakan oleh kelengahan pengguna sebenarnya tidak ada, tetapi hal ini bisa diatasi apabila pengguna berhati – hati dalam membuka suatu situs atau *file* pada komputernya. Lebih baik memastikan terlebih dahulu apakah ada *malware* pada *file* yang akan dibuka atau pada situs yang akan dibuka. Lebih baik bila kita mempunyai suatu *software anti-virus* pada komputer kita, dan *anti-virus* tersebut haruslah *up-to-date*, karena bila ada virus baru sedangkan *anti-virus* yang kita punya tidak *up-to-date* maka *anti-virus* kita tidak dapat mendeteksi *virus* terbaru. Namun ada masalah yang sangat terkait dengan penggunaan *anti-virus* yang dapat membuat pengguna merasa tidak nyaman. Contohnya adalah kita harus selalu meng-*update anti-virus* tersebut agar dapat mengenali *virus* terbaru, dengan begitu berarti kita harus mempunyai koneksi yang terhubung dengan *internet* dan kemudian harus menunggu *update* dari *anti-virus* tersebut. Selain itu, kita harus ruti melakukan *scanning* dalam komputer kita agar keberadaan *malware* dalam komputer kita dapat terdeteksi oleh *anti-virus* yang kita gunakan. Hal ini mungkin tidak nyaman bagi beberapa pengguna, namun jika ingin memperkuat keamanan komputer kita, kenyamanan kita harus dikorbankan sedikit.

Sistem keamanan pada komputer bisa kita tingkatkan dengan menggunakan *software – software* pendukung seperti *anti-virus, firewall, spyware blocker, adware blocker*, dan *software* lain yang sejenis. Dari tadi kita sudah melihat *anti-virus* dan sebagainya. Sebenarnya apa sih *anti-virus* itu? *Anti-virus* adalah suatu *program* komputer yang digunakan untuk mengidentifikasi, mengkarantina, dan membuang *virus* dan *malware* lainnya yang ada pada komputer kita. *Anti-virus* biasanya menggunakan 2 teknik berikut untuk melakukan hal diatas, yaitu :

a. Meng-*scan file* untuk mengecek apakah ada *virus* dalam *file* tersebut yang cocok dalam kamus *virus* yang dipunyai oleh *anti-virus* tersebut.
b. Mengidentifikasi kebiasaan dari *program* komputer dimana ada kemungkinan telah terinfeksi. Seperti analisis terhadap data, *port monitoring*, dan metode lainnya.

Contoh *anti-virus* yang paling sering digunakan dan diketahui sebagai *anti-virus* yang *powerful* adalah : Kaspersky Anti Virus, Norton Anti Virus, McAfee Anti Virus, TrendMicro PC-CILIN, Panda Platinum Anti Virus, dan masih banyak *vendor – vendor anti-virus* lainnya walau tidak di-rekomendasi oleh Microsoft. Jika untuk menggunakan *anti-virus* yang disebut diatas kita harus membeli yang asli (jika tidak ingin menggunakan *program* bajakan), ada pula *vendor – vendor*

anti-virus yang gratis (*free version)* seperti yang paling sering digunakan adalah AVG Anti Virus dan Avast! Anti Virus.

Penggunaan *firewall* juga penting, untuk membatasi siapa saja dan program apa saja yang bisa berjalan dalam komputer kita. Penggunaan *firewall* penting untuk mengatasi *malware trojan*, karena jika ada orang lain yang mengakses komputer kita tanpa ijin, maka hak akses-nya akan di-blokir oleh *firewall* tersebut. Contoh *firewall* yang paling sering digunakan adalah Zone Alarm Firewall dan Tiny Personal Firewall. Keduanya dapat digunakan secara gratis, tetapi bila kita menggunakan yang versi gratis, maka ada fitur – fitur yang tidak bisa digunakan.

Spyware blocker dan *adware blocker* biasanya digunakan untuk menghapus *spyware / adware* yang sudah terinfeksi dalam sistem komputer kita, maupun memblok jika ada *spyware* atau *adware* yang ingin menginfeksi sistem komputer kita.

V. KESIMPULAN

Dari analisis dan pembahasan diatas, dapat disimpulkan bahwa *computer security* sangatlah penting untuk melindungi sistem komputer terutama untuk melindungi data – data penting yang tersimpan di dalamnya. Berbagai jenis *malware* seperti *infectious malware (computer virus* dan *worm)*, *concealment malware (trojan horse)*, dan *malware for profit* yang terbagi lagi menjadi *spyware, spammer virus, botnets,* dan *keylogger* bisa dikatakan *sangat* berbahaya karena dapat menyebabkan resiko yang sangat tinggi terhadap keamanan komputer itu sendiri. Penyebab komputer terkena serangan *malware* adalah karena pengguna dalam melakukan *copy* data ataupun *file* tanpa melakukan *scan* pada *file* yang bersangkutan. Selain itu juga kurangnya kemampuan komputer tersebut dalam melakukan proteksi pada seluruh *file* yang ada di *hard disk*. Masalah lainnya dikarenakan sistem operasi yang digunakan oleh pemakai memiliki lubang-lubang yang harus ditutupi dengan cara meng-*update* dari situs berdasarkan sistem operasi yang digunakan.

Dari berbagai permasalahan yang terjadi akibat *virus* yang menyerang keamanan komputer tersebut, bukan tidak mungkin terdapat beberapa solusi yang diharapkan dapat menindaklanjuti permasalahan tersebut, diantaranya adalah dengan menggunakan *program anti-virus, firewall, spyware removal (blocker),* dan *adware removal (blocker)*, maupun dengan *program – program* pendukung lainnya. Selain itu para pengguna komputer sangat diharapkan untuk berhati – hati dalam membuka suatu *file* atau meng-*install* suatu *software* (dalam hal ini yaitu dengan memperhatikan baik – baik apa saja yang kita *install* termasuk membaca '*Terms and Agreement*' yang tersedia), selain itu juga jangan sembarangan dalam membuka situs – situs di internet.

Jika ada sesuatu yang aneh terjadi pada komputer kita, belum tentu ada *virus* di sistem komputer kita, karena bila ada sistem yang berubah / terhapus secara tidak sengaja oleh pengguna, akan menyebabkan komputer tidak bekerja dengan baik dan sering kali muncul pesan *error*. Tetapi jika keanehan itu bersifat hilang-nya *file* secara tiba – tiba, komputer *restart* dengan sendirinya, ataupun jika ada folder sistem yang menghilang secara tiba – tiba, maka kemungkinan besar penyebabnya adalah adanya *malware* pada sistem komputer kita. Untuk itu kita harus mempunyai *anti-virus* dengan *update* terbaru agar bisa mendeteksi semua tipe *malware* yang terdaftar dalam *virus definition* pada *anti-virus* tersebut, dan jangan lupa untuk melakukan *scan* rutin tiap hari atau tiap minggu terutama apabila anda suka menggunakan *storage disk external* yang digunakan juga pada komputer lain.

DAFTAR PUSTAKA

[1] http://en.wikipedia.org/wiki/Computer_security
[2] http://www.howstuffworks.com/virus.html
[3] http://en.wikipedia.org/wiki/Computer_worm
[4] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
[5] http://en.wikipedia.org/wiki/Malware
[6] http://en.wikipedia.org/wiki/Adware
[7] http://en.wikipedia.org/wiki/Spyware
[8] http://www.microsoft.com/athome/security/viruses/intro_viruses_what.mspx
[9] http://www.faqs.org/faqs/computer-virus/new-users/
[10] http://www.cert.org/other_sources/viruses.html
[11] http://en.wikipedia.org/wiki/Spam_%28electronic%29
[12] http://en.wikipedia.org/wiki/Keystroke_logging
[13] http://en.wikipedia.org/wiki/Antivirus_software
[14] http://www.webopedia.com/TERM/f/firewall.html