

KEAMANAN KOMPUTER DAN JARINGAN

--VIRUS, TROJAN HORSE, WORM, SPYWARE, ANTIVIRUS—



Tim Penyusun:

- **Dedi Kurniawan (D1A.06.012)**
- **Muhammad Bahri (D1A.06.011)**
- **Gingin Ginanjar Rahayu (D1A.06.010)**
- **Yadi Supriyadi (D1A.06.013)**

**MAHASISWA FAKULTAS ILMU KOMPUTER
UNIVERSITAS SUBANG**

UNIVERSITAS SUBANG

JL. RA. KARTINI KM. 3 Telp. (0260) 411415 Fax. 415677

SUBANG

Abstraksi

Dengan meningkatnya tingkat intelegensia manusia dalam perkembangannya, telah melahirkan sesuatu yang baru, yang berguna bagi dunia juga melahirkan yang merugikan dunia itu sendiri. Perkembangan teknologi informasi dan komunikasi (ICT) telah merubah paradigma manusia akan kemudahan penggunaan teknologi beserta penerapannya.

Penerapan teknologi tersebut banyak digunakan di perusahaan-perusahaan besar, maupun dirumah. Namun, adakalanya pihak tertentu memanfaatkan berbagai kemajuan IPTEK tersebut dengan "memajukan" sesuatu yang baru, yang justru *against* sekaligus mendukung untuk terus berkembang lagi.

Virus komputer, merupakan salah satu *script code* yang dapat mendatangkan kerugian bagi pihak yang perangkat teknologinya dijangkiti oleh virus ini. Sebagaimana virus dalam dunia kesehatan, virus ini pun seolah-olah mempunyai pengembangan biologis dengan cara meng-*copy* sendiri file yang dapat memperlambat kinerja komputer dalam memproses data atau informasi didalamnya, sehingga menimbulkan *crash* pada komputer tersebut dan beresiko kehilangan data yang telah dan sedang diproses.

Kata Pengantar

Perkembangan virus komputer dewasa ini sangat pesat, seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Berbagai motif yang digunakan oleh para pembuat virus dalam menjalankan aksinya, merupakan salah satu faktor penyebab terjadinya perkembangan virus komputer ini.

Namun, belakangan kita mengetahui ragam virus yang beredar dimasyarakat dengan jenis dan sasaran yang bervariasi. Sehingga menuntut *user* untuk terus menjaga keamanan data dan informasi yang terdapat di komputernya. Karena virus yang ditimbulkan dapat menyebabkan terhapusnya data dan informasi yang ada di komputer tersebut. Selain virus, dikenal pula ragam malware lainnya, seperti Trojan Horse, Worm, Spyware, dan masih banyak lagi.

Pada karya tulis kali ini, penyusun akan mencoba untuk memberikan sebuah gambaran singkat, kenapa virus komputer itu bisa tersebar, dan apa dampak yang ditimbulkannya. Serta bagaimana caranya menanggulangi ragam malware tersebut.

Tidak lupa, penyusun ucapkan banyak terima kasih kepada semua unsur yang terlibat dalam pembuatan karya tulis ini. Sehingga, karya tulis ini dapat segera dirampungkan sesuai dengan *dateline* yang telah ditentukan.

Tim Penyusun

Daftar Isi

Abstrak.....	ii
Kata Pengantar.....	iii
Daftar Isi.....	iv
BAB I VIRUS KOMPUTER	
1.1 Definisi Virus Komputer	1
1.2 Perbedaan Virus, Worm, dan Trojan Horse	1
1.2.1 Trojan Horse.....	1
1.2.2 Worm.....	2
1.2.3 Spyware.....	3
1.3 Dampak yang Ditimbulkan Oleh Virus	4
1.4 Letak Resiko Virus	6
1.5 Target Virus (File-File yang Rentan)	6
1.6 Sejarah Virus dan Malware Lainnya	8
1.7 Mobile Technology, Sasaran Virus Masa Depan	15
1.7.1 Telepon Selular.....	15
1.7.2 Palmtop atau PDA.....	16
1.7.3 SmartPhone.....	16
1.7.4 Teknologi Bluetooth.....	17
1.8 Mencegah Virus.....	18
BAB II PROGRAM ANTIVIRUS	
2.1 Definisi Antivirus	19
2.2 Perkembangan Antivirus	21
2.3 Antivirus untuk SmartPhone	21
3 Daftar Pustaka.....	22

LAMPIRAN

Biodata Tim Penyusun

BAB I

VIRUS KOMPUTER

1.1 Definisi Virus Komputer

Virus komputer adalah sebuah program kecil yang bisa menggandakan dirinya sendiri dalam media penyimpanan suatu komputer. Formalnya adalah sebagai berikut: *“A program that can infect other programs by modifying them to include a slightly altered copy of itself. A virus can spread throughout a computer sistem or network using the authorization of every user using it to infect their programs. Every programs that gets infected can also act as a virus that infection grows (Fred Cohen).*

Virus juga mampu, baik secara langsung ataupun tak langsung, menginfeksi, mengkopi maupun menyebarkan program file yang bisa dieksekusi maupun program yang ada di sektor dalam sebuah media penyimpanan (Hardisk, Disket, CD-R). Virus juga bisa menginfeksi file yang tidak bisa dieksekusi (file data) dengan menggunakan macros (program sederhana yang biasanya digunakan untuk melakukan suatu perintah). Intinya adalah kemampuan untuk menempel dan menulari suatu program.

Virus bukanlah sesuatu yang terjadi karena kecelakaan ataupun kelemahan perangkat komputer karena pada hakikatnya, semua virus merupakan hasil rancangan intelegensi manusia setelah melalui beberapa percobaan terlebih dahulu layaknya eksperimen-eksperimen ilmiah di dalam bidang-bidang lainnya.

1.2 Perbedaan virus, worm, dan Trojan horse

1.2.1 Trojan Horse

Trojan horse adalah program yang kelihatan seperti program yang valid atau normal, tetapi sebenarnya program tersebut membawa suatu kode dengan fungsi-fungsi yang sangat berbahaya bagi komputer Anda. Sebagai contoh, virus DLoader-L datang dari attachment e-mail dan dianggap sebagai sebagai suatu update program dari Microsoft untuk sistem operasi Windows XP. Jika Anda menjalankannya maka dia akan mendownload program dan akan memanfaatkan komputer Anda untuk menghubungkan komputer Anda ke suatu website tertentu. Targetnya tentu saja untuk membuat website tadi menjadi overload dan akhirnya tidak bisa diakses dengan benar oleh pihak lain. Ini sering dinamakan dengan serangan denial of service atau DoS.

Trojan tidak dapat menyebar secepat virus karena trojan tidak membuat copy dari dirinya sendiri secara otomatis. Tapi sejalan dengan perkembangan virus, maka trojan horse bisa bekerjasama dengan virus dalam hal penyebarannya. Virus dapat melakukan download terhadap trojan yang merekam keystroke keyboard Anda atau mencuri informasi yang ada pada komputer Anda. Di sisi lain, trojan juga digunakan untuk menginfeksi suatu komputer dengan virus.

Trojan horse tidak memiliki kemampuan untuk menggandakan dirinya ke program lain. Namun demikian, program ini tidak kalah berbahaya jika dibandingkan dengan program virus komputer.

Trojan horse umumnya dikemas dalam bentuk sebuah program yang menarik. Namun dibalik 'pesona' software tersebut, tersembunyi fungsi lain untuk melakukan perusakan. Pengguna komputer yang mendapatkan file ini umumnya akan terpancing untuk menjalankannya. Akibatnya tentu fatal, karena dengan demikian si pengguna telah menjalankan rutin-rutin perusak yang dapat mendatangkan malapetaka pada sistem komputernya.

Trojan pertama muncul pada tahun 1986 dalam bentuk program shareware yang dikenal dengan nama PC-Write. Oleh karena itu, user harus memastikan shareware atau freeware-nya bebas dari trojan dengan cara memasang sejenis firewall atau antivirus ke dalam sistem komputer anda.

1.2.2 Worm

Sumber malapetaka lain yang mirip dengan virus, namun tidak bisa dikategorikan sebagai virus, adalah worm. Worm adalah program yang dapat menduplikasi diri tanpa menginfeksi program-program lainnya. Worm tidak memerlukan carrier, dalam hal ini program atau suatu dokumen. Worm biasa menyebar melalui pertukaran data antar hardisk, disket, maupun e-mail. Penyebaran melalui e-mail biasanya berupa sebuah attachment yang kecil. Pengguna yang tertarik akan menjalankan program tersebut. Selanjutnya, tanpa basa-basi, si program akan langsung melakukan aksinya. Worm akan menggandakan diri dengan mengirimkan file-nya secara otomatis melalui attachment ke setiap alamat yang ada dalam address book pada mail manager korban.

Umumnya worm tidak bersifat merusak, namun demikian selain mengakibatkan kejengkelan di pihak korban, serangan worm dapat sangat berbahaya bagi mailserver. Berjangkitnya worm menyebabkan beban kerja mailserver melonjak drastis hingga dapat mempengaruhi performanya.

Dan tidak hanya untuk mailserver, bahkan komputer pribadi kita pun bisa dijadikan sasarannya. Hal ini terjadi karena worm mampu menduplikasikan dirinya sendiri di dalam memori komputer dalam jumlah yang sangat banyak. Sekarang bayangkan jika worm menduplikasi dirinya secara serentak, 'bakal lemot deh komputer'.

Worm umumnya berbentuk file executable (berekstensi .EXE atau .SCR), yang terlampir (attach) pada e-mail. Namun demikian, ada beberapa jenis worm yang berbentuk script yang ditulis dalam bahasa Visual Basic (VBScript). Sasaran serangan worm jenis ini terutama adalah perangkat lunak e-mail Microsoft Outlook Express, tapi bukan berarti aplikasi yang lain sudah pasti kebal dengan semua jenis worm.

1.2.3 Spyware

Selain Virus, Trojan Horse dan Worm, ada juga yang disebut dengan Spyware. Spyware adalah suatu aplikasi yang memungkinkan para pemasang iklan untuk mendapatkan informasi mengenai kebiasaan pengguna komputer dimana spyware tersebut terpasang. Program spyware ini sebenarnya bukanlah suatu virus. Anda tidak dapat menyebarkan ke komputer yang lain. Tetapi spyware terkadang memiliki efek-efek lain yang tidak terduga. Anda bisa saja mendapatkan spyware ketika Anda mengakses suatu situs tertentu. Suatu pesan pop-up biasanya akan muncul dan menyuruh Anda untuk mendownload program yang "kelihatannya" Anda butuhkan, atau terkadang program spyware ini bisa secara otomatis terdownload tanpa Anda sadari.

Spyware akan jalan di komputer Anda dan akan mencatat semua aktivitas Anda (misalnya mencatat situs apa saja yang Anda kunjungi) dan akan melaporkannya kepada pihak lain, dalam hal ini pihak pemasang iklan. Efek lainnya adalah mengganti halaman home pada web browser Anda dengan suatu alamat situs tertentu atau bahkan juga ada yang memiliki efek untuk men-dial modem ke nomor 0900 (premium call). Aktivitas spyware ini jelas

akan memakan *resource* pada komputer Anda dan dapat memperlambat performa dari komputer Anda.

Beberapa software anti-spyware saat ini sudah dapat mendeteksi adanya spyware pada komputer Anda dan bisa menghilangkannya secara otomatis. Contohnya adalah fitur anti-spyware pada aplikasi System Mechanic

1.3 Dampak yang Ditimbulkan Oleh Virus

- Memperlambat e-mail

Virus dapat menyebar melalui e-mail, seperti virus Sobig, dan mampu untuk membuat trafik e-mail yang sangat besar yang tentu saja akan membuat server menjadi lambat atau bahkan menjadi crash. Bahkan jika hal tersebut tidak sampai terjadi, perusahaan yang merasa terganggu dengan insiden ini toh juga akan mematikan servernya.

- Mencuri data konfidental

Worm Bugbear-D contohnya, mampu merekam keystroke keyboard Anda, termasuk password dan lain sebagainya. Rekaman tadi biasanya akan dikirim ke si pembuat virus untuk dimanfaatkan lebih lanjut.

- Menggunakan komputer Anda untuk menyerang suatu situs

MyDoom contohnya, dia menginfeksi banyak komputer di seluruh dunia untuk menyerang situs SCO dengan traffic data yang sangat besar. Ini akan membuat situs tersebut akan terbebani luar biasa dan akhirnya akan crash dan tidak bisa melayani pengguna lainnya. Ini biasa dinamakan dengan denial of service.

- Membiarkan orang lain untuk membajak komputer Anda

Beberapa virus menempatkan trojan backdoor pada komputer dan ini akan membuat si pembuat virus dapat terhubung ke komputer tersebut secara diam-diam dan bisa dimanfaatkan lebih lanjut sesuai dengan keinginannya.

- Merusak data
Virus Compatable contohnya, dapat membuat perubahan pada data yang Anda simpan pada dokumen MS Excel.
- Menghapus data
Virus Sircam contohnya, berusaha untuk menghapus atau meng-overwrite hardisk Anda pada suatu waktu tertentu yang tidak terduga.
- Men-disable hardware
Virus CIH atau Chernobyl contohnya, berusaha untuk meng-overwrite chip BIOS pada tanggal 26 April dan akan membuat komputer Anda menjadi tidak berfungsi.
- Menimbulkan hal-hal yang aneh dan mengganggu
Virus worm Netsky-D contohnya, dapat membuat komputer berbunyi beep secara spontan atau tiba-tiba untuk beberapa jam lamanya.
- Menampilkan pesan tertentu
Virus Cone-F contohnya, akan menampilkan pesan berbau politik jika bulan menunjukkan bulan Mei.
- Merusak kredibilitas Anda
Jika virus mem-forward dirinya sendiri dari komputer Anda ke komputer pelanggan Anda atau komputer rekan bisnis Anda, maka hal ini akan merusak reputasi Anda sebagai suatu organisasi dan mereka akan tidak mau lagi melanjutkan hubungan bisnis dengan Anda atau malah menuntut kompensasi dari pihak Anda.
- Membuat malu Anda
Virus PolyPost contohnya, akan memposting dokumen dan nama Anda pada newsgroup yang berbau pornografi.

1.4 Letak Resiko Virus

- **Program dan dokumen**

Program komputer dan juga dokumen dapat terinfeksi oleh virus. Ketika Anda men-sharing program atau dokumen tadi kepada rekan-rekan Anda yang lain, maka hal ini akan membuat penyebaran virus akan semakin luas apalagi jika menyebar melalui jaringan LAN kantor Anda atau bahkan melalui internet.

- **Internet**

Anda bisa saja men-download program atau dokumen yang sudah terinfeksi virus dari internet. Celah keamanan pada komputer Anda dapat membuat virus untuk memanfaatkannya. Virus dapat menular ke komputer Anda melalui internet secara otomatis tanpa Anda melakukan apa-apa sebelumnya.

- **E-mail**

E-mail yang Anda terima setiap hari dapat saja membawa virus melalui attachment. Begitu Anda menjalankan program atau dokumen yang ada pada attachment tadi, maka komputer Anda akan terinfeksi oleh virus. Beberapa e-mail bahkan dapat mengandung script berbahaya yang akan dijalankan begitu Anda melakukan preview terhadap e-mail atau membaca isi dari e-mail Anda.

- **CD atau disket**

Disket dapat membawa virus pada boot sector-nya. CD atau disket juga bisa berisi program yang sudah terinfeksi oleh virus.

1.5 Target Virus (File-File yang Rentan)

- **Program**

Beberapa virus mampu untuk menginfeksi program komputer. Jika Anda menjalankan program yang sudah terinfeksi virus tadi, maka kode virus secara otomatis juga akan dijalankan pertama kali. Virus-virus jenis ini muncul pada saat awal-awal munculnya virus di dunia komputer dan sampai sekarang masih merupakan ancaman yang serius apalagi dengan perkembangan internet yang mampu untuk mendistribusikan program dengan cepat ke seluruh dunia.

- **Dokumen**

Word processing atau spreadsheet, seperti MS Word atau MS Excel, seringkali menggunakan macro untuk mengotomatisasi suatu pekerjaan. Beberapa virus memanfaatkan fasilitas macro ini untuk menyebarkan dirinya sendiri ke dokumen yang lainnya. Jika Anda menjalankan dokumen yang mengandung virus macro ini, maka dia akan meng-copy dirinya ke startup program yang membuka dokumen tersebut dan akhirnya bisa menuluri dokumen lainnya yang masih bersih dari virus.

- **Boot sector**

Ketika Anda menghidupkan komputer, maka komputer akan mengakses suatu bagian pada disk yang disebut dengan "boot sector" dan akan menjalankan program yang nantinya akan memulai sistem operasi. Pada jaman awal-awalnya virus komputer, seringkali area boot sector ini ditumpuki dengan kode virus, sehingga ketika komputer dinyalakan dan mengakses boot sector, maka kode virus secara otomatis akan dijalankan pula.

- **Virus e-mail**

Kebanyakan virus e-mail ini sangat tergantung dari user yang mengklik dokumen atau program yang ada pada attachment e-mail. Ini akan menimbulkan virus untuk mem-forward dokumen yang terinfeksi tadi kepada alamat e-mail yang lainnya. Virus Netsky sebagai contoh, mampu mencari file-file dalam komputer Anda yang berisi alamat e-mail (misalnya HTML file atau file dalam format EML), dan akan menggunakan program e-mail yang ada pada komputer Anda untuk mengirimkan dokumen yang terinfeksi ke alamat-alamat e-mail yang sudah didapat tadi.

Beberapa virus lainnya seperti Sobig-F bahkan sudah tidak memerlukan program e-mail pada komputer Anda untuk mengirimkan e-mail, tetapi mereka memiliki SMTP engine sendiri untuk mengirimkan e-mail. E-mail virus ini bisa menguasai komputer Anda atau bahkan mencuri data. Tetapi target utama dari jenis virus e-mail ini biasanya akan menimbulkan trafik e-mail yang sangat besar dan membuat server menjadi crash. Sekali lagi hati-hatilah terhadap attachment pada e-mail Anda. Bahkan attachment dengan

ekstensi .txt juga dapat berbahaya karena seringkali dibelakangnya masih ada ekstensi lagi misalnya .vbs yang dapat berisi script dari virus.

1.6 Sejarah virus dan malware lainnya

Meskipun banyak pihak yang bersepakat bahwa worm dan trojan tidak dapat dikategorikan sebagai virus, namun dalam sejarahnya, penyampaian riwayat perjalanan virus akan selalu disertai oleh cerita-cerita tentang kemunculan dan aksi-aksi dari malware lainnya, yaitu worm dan trojan. Hal ini memang tidak dapat dihindari karena kedua ‘makhluk’ tersebut lahir sebagai imbas dari kemampuan virus sendiri.

1981 : Virus Pertama di komputer (nenek moyang virus)

Pada tahun 1981, program yang bernama Elk Cloner muncul di komputer Apple II. Program ini (pada tahun ini istilah computer virus belum ditemukan) menampilkan enam baris kalimat di monitor komputer seperti berikut :

It will get on your disk

It will infiltrate your chips

Yes it's Cloner!

It will stick to you like glue

It will modify ram too

Send in the cloner!

1983 : Dokumentasi computer virus pertama kali

Pada tahun 1983, ujicoba dokumentasi virus pertama kali dilakukan oleh Fred Cohen. Cohen adalah seorang mahasiswa S3 sekaligus peneliti yang secara teoretis dan dengan berbagai eksperimen ilmiahnya mampu memberikan pengertian dan pemahaman kepada dunia bahwa akan ada ‘makhluk baru’ di sekitar kita yang sangat potensial menjadi ‘pengacau’ di dalam perkembangan abad komputer dan telekomunikasi.

1986 : Virus pertama di PC

‘The Brain’ adalah nama untuk virus yang pertama kali diketahui menjangkiti PC. Virus ini dibuat oleh dua orang bersaudara asal Pakistan, Basit and Amjad, pada tahun 1986. Virus ini menjangkiti disket yang dimasukkan pada PC bersistem operasi MS-

DOS. Setiap disket yang sudah terinfeksi akan memiliki volume label : “ © Brain ”. ‘The Brain’ juga kerap disebut sebagai virus stealth komputer yang pertama karena virus ini mampu menguasai tabel interrupt pada DOS (Interrupt interceptor). Virus ini berkemampuan untuk mengendalikan instruksi-instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya baik secara penuh ataupun ukurannya.

1987 : Virus menyerang ekstensi *.COM

Tahun ini merupakan tahunnya virus file. Varian ini secara khusus menyerang semua file yang berekstensi *.COM. File yang umum diserang adalah command.com dengan subyek penyerang bernama virus Lehigh. Selain menyerang *.COM, virus pada masa itu juga telah mampu menyerang file *.EXE, seperti virus Suriv-02. Selain virus, worm juga tidak mau ketinggalan menyebarkan serbuan virus ke sistem komputer ketika itu. Tercatat dalam sejarah bahwa pada tahun ini muncul istilah “The IBM Christmas Worm” sebagai imbas dari banyaknya mainframe milik IBM yang terserang worm.

1988 :Virus untuk Macintosh, worm untuk ARPANET, antivirus untuk ‘the brain’

Pada tahun ini macintosh mulai terjangkit oleh virus yang bernama MacMag dan The Scores. Itu masih termasuk kabar baik. Kabar buruknya adalah rontoknya 6000 komputer yang berada dalam jaringan ARPANET karena ulah ‘seekor’ worm karya Robert Morris (usianya baru 23 tahun ketika itu).

Worm-nya bekerja dengan cara menduplikasikan dirinya sendiri lalu mengendap di dalam memori komputer. Lucunya, worm tersebut ia buat hanya karena ingin membunuh rasa bosan. Akhirnya, penjara menjadi rumahnya selama 3 tahun plus denda sebesar \$ 10.000,00. Kabar buruk lainnya adalah lahirnya ‘Jerusalem’ dan ‘Cascade’. Virus Jerusalem hanya aktif/hidup pada tanggal 13 hari jum’at (Friday The 13th) dan menginfeksi dua ekstensi sekaligus, yaitu *.EXE dan *.COM.

Hebatnya, semua komputer yang terinfeksi akan kehilangan program-program mereka jika dijalankan pada tanggal tersebut. Sementara cascade yang ditemukan oleh orang Jerman merupakan virus pertama yang terenkripsi (encrypted virus) sehingga tidak

dapat diubah atau dihilangkan untuk zaman itu. Kecuali oleh orang yang mengetahui kode enkripsi-balik (decode) tentunya. Contohnya si pembuat virus itu sendiri.

1989 : Trojan AIDS dan Dark Avenger

Trojan AIDS menyebar sebagai program yang dapat menahan data informasi AIDS (Acquired Immuno Deficiency Syndrome) di dalam komputer yang dijangkitinya. Mungkin berguna jika berada di hardisk para dokter maupun praktisi kesehatan, tapi lain masalahnya dengan matematikus maupun praktisi perbankan.

Pada bulan september tanggal 17, Washington Post melaporkan tentang sebuah virus yang mereka sebut dengan bahasa jurnalisnya : “virus yang hidup dan menghancurkan pada tanggal 13 hari jum’at telah kabur”. Virus ini bekerja layaknya Jerussalem, namanya adalah DataCrime. Model penyerangan gaya baru diperkenalkan oleh virus Dark Avenger. Virus ini dirancang untuk menghancurkan sistem komputer secara perlahan-lahan. Jadi, pada awalnya pengguna tidak akan menyadari bahwa komputer mereka terserang virus, hingga tiba saat waktunya komputer akan berjalan semakin lambat, lambat, dan lambat.

Pada bulan oktober di Israel muncul virus yang disebut Frodo. Virus ini merupakan virus yang diprogram untuk merusak harddisk (harddrive) yang berjalan pada tanggal 22 September atau setelahnya pada tahun berapapun.

1992 : Toolkit pembuat virus

The Dark Avenger Mutation Engine (DAME) menjadi toolkit pembuat virus pertama yang dapat mengubah virus biasa menjadi virus polymorphic. Selain DAME lahir juga VCL (Virus Creation laboratory) yang menjadi perangkat pembuat virus pertama. Pada bulan Maret virus Michaelangelo muncul, berita-berita yang disebar oleh media mengenai virus ini membuat penjualan antivirus meningkat tajam. Statistik mencatat bahwa sudah ada sekitar 1300 virus pada tahun ini. Berarti meningkat 420% sejak bulan Desember 1990.

1993 : Virus yang baik dan Satan Bug

Cruncher sering dianggap sebagai virus yang baik karena ia mengompres setiap file yang diinfeksi. Jadi, ia dianggap juga sebagai penyelamat kapasitas storage.

Sementara itu, di lain tempat sebuah kejutan besar terjadi. Sang pembuat virus The Satan Bug yang penangkapannya dilakukan oleh FBI menggunakan bantuan para vendor antivirus ternyata hanyalah seorang anak kecil.

1994 : Good Times yang membuat bad times ; Hoax pertama

Good Times adalah virus yang disebarkan melalui e-mail dengan subject seperti namanya sendiri. Dalam isi pesannya ia menyebutkan bahwa hanya dengan membaca atau melihat pesan bersubject “good times” pada komputer maka isi hardisk dari komputer tersebut akan lenyap dan bahkan merusak processor. Setelah diuji dengan cermat, ternyata isi pesan tersebut hanyalah berita bohong (hoax) saja. Good times sejatinya hanyalah virus yang mereplikasikan dirinya layaknya virus-virus lain.

1995 : Windows 95 dan virus Macro pertama

Munculnya windows 95 banyak membuat vendor antivirus khawatir kalau nantinya produk mereka bakal tidak berfungsi lagi dan tidak ada yang membeli. Namun, virus macro pertama muncul, namanya Concept. Virus ini memang tidak menyerang DOS namun menyerang aplikasi word processor paling terkenal saat itu, yaitu MS-Word. Vendor antivirus bak mendapat buah simalakama, satu sisi mereka senang, sisi lain mereka tidak. Karena musuh mereka bertambah lagi.

1996 : virus untuk windows 95, linux, dan Excel

Setahun setelah kemunculannya, Concept semakin populer diseantero dunia. Ms Excel akhirnya juga kebagian virus dengan adanya Laroux. Tidak ketinggalan, virus Boza dan Staog menjadi virus pertama buat Windows 95 dan open source OS ; Linux. Setelah diusut ternyata pembuat Boza dan Staog adalah satu kelompok yang sama.

1998 : Virus Java, Back Orifice, dan Solar Sunrise

Strange Brew adalah virus yang menyerang file java untuk yang pertama kalinya, tapi daya rusaknya tidak terlalu ‘membanggakan’. Pada tahun ini trojan yang melegenda hingga sekarang, Back Orifice, merupakan tool kendali jarak jauh (remote administration) yang mengizinkan seseorang mengambil ahli komputer orang lain via jaringan, baik jaringan lokal maupun jaringan internet. Virus macro untuk Access mulai muncul tahun ini juga.

Salah satu kejadian yang paling menggemparkan pada tahun ini adalah ketika dua orang remaja asal California berhasil menyusup dan mengendalikan sistem komputer milik Departemen pertahanan USA, kantor-kantor pemerintahan, dan lembaga-lembaga swasta publik. Kecelakaan ini populer dengan istilah ‘Solar Sunrise’ karena OS yang banyak dipakai oleh komputer yang terserang tersebut adalah Sun Solaris. Selain itu, tahun ini juga merupakan tahun kemunculan Chernobyl, sebuah virus yang merusak sistem penyimpanan hardisk dan mampu mengacaukan sistem. Di Cina saja, kerugian mencapai 120 juta dollar AS.

Untungnya, virus ini hanya menyerang OS Windows dan tidak menyerang OS macam Unix dan Novell Netware. Jika saja kedua OS belakangan juga terinfeksi maka kerugian yang terjadi bisa lebih besar karena Unix dan Netware banyak digunakan di sektor perbankan, pemerintahan, sekuritas, penerbangan, dan telekomunikasi.

1999 : Please welcome Melissa

Tahun ini benar-benar menjadi milik Melissa, virus macro yang memanfaatkan MS Word, Outlook Express dan jaringan internet dalam persebarannya. Melissa menjadi virus yang menyebar paling cepat dibanding virus-virus sebelumnya dan tentu saja menjadi katalis penjualan antivirus di seluruh dunia.

Bubble Boy muncul dan menjadi virus pertama yang tidak bergantung pada user untuk melakukan aksinya. Jadi, ketika seorang penerima attachment Bubble Boy ini membuka program mail manager-nya seperti Ms Outlook, maka sang virus tidak harus menunggu untuk dibuka dahulu file attachment-nya. Virus Corner muncul melengkapi deretan malware yang gemar menjangkiti produk-produk Microsoft. Kali ini yang menjadi sasaran adalah Ms Project. Tristate menjadi virus pertama yang mampu menginfeksi tiga varian Ms Office sekaligus, yaitu Ms Word, Excel, dan Power point.

2000 : waktunya katakan cinta dengan ‘I Love You’

Seorang pemuda Filipina diketahui sebagai pembuat virus ‘I Love You’. Modus kerja virus ini menyerupai Melissa tetapi lebih canggih dan lebih menghancurkan dibanding Melissa sendiri. Jika Melissa hanya mengambil 50 daftar e-mail yang ada di komputer yang terjangkiti kemudian mengirimkannya kepada komputer lain melalui internet,

maka I Love You tidak hanya mengambil 50, tetapi semua. Hebatnya lagi, semua informasi tentang e-mail yang diambil dari address book komputer tersebut, seperti username dan password akan dikirimkan ke alamat sang penulis virus. Plus kemampuan menghapus file-file yang berekstensi *.MP3, *.MP2, dan *.JPG.

2001 : Kournikova, Code Red, dan Nimda

Virus 'Anna Kournikova' yang menggunakan gambar petenis muda bersinar dari Rusia sebagai umpannya bekerja dengan cara mengirimkan dirinya sendiri ke e-mail yang ada di Address Book Ms Outlook. Munculnya virus ini membuat para analis security khawatir bahwa jangan-jangan di luar sana para pembuat virus tidak perlu lagi harus bersusah payah untuk memikirkan algoritma yang rumit dalam proses pembuatan virus dikarenakan oleh tersedianya tool-tool pembuatan virus yang mudah didapat di internet. Code Red membuat dunia heboh ketika daya (resource) semua komputer yang berhasil dijangkitinya dapat ia gunakan untuk membuat jatuhnya sistem pada website gedung putih (White House). Kerugian yang dihasilkan oleh virus ini di USA mencapai sekitar \$ 2 Milyar. Padahal, komputer yang diserang oleh virus tersebut hanyalah komputer yang menggunakan windows 2000 server dan windows NT sebagai OS-nya.

Tepat sehari setelah kejadian penghancuran gedung WTC pada 11 September 2001 muncullah Nimda. Virus ini dianggap sebagai salah satu virus yang paling pintar di dalam riwayat sejarah virus karena ia memiliki lima jenis cara/metode untuk menginfeksi sistem dan mereplikasi dirinya sendiri.

Pada tahun ini sang penulis virus Melissa, David L. Smith (33 tahun), akhirnya berhasil ditangkap dan dimasukkan ke penjara federal Amerika Serikat selama 20 tahun.

2002 : worm Klez dan para superstar

Klez, worm ganas yang menyebar melalui internet. Uniknya, setelah dia mengirimkan kopi dari dirinya sendiri kepada semua korbannya, yaitu semua e-mail yang berada dalam folder Ms Outlook, Klez kemudian membuat hidden Copy dari file asli yang dijangkitinya. Selain itu, worm populer ini juga mampu menonaktifkan beberapa produk antivirus yang sudah terinstall terlebih dahulu di komputer korban. Melanjutkan sukses virus 'Anna kournikova' yang mampu menghebohkan dunia

maya sebelumnya, hadirlah kemudian beberapa virus yang menggunakan nama selebritis hollywood sebagai 'detonator'-nya. Selebritis tersebut antara lain, Britney Spears, Shakira, dan Jennifer Lopez.

2003 : Slammer dan Sobig, lagi-lagi cacing, worm...

worm 'Slammer' sejatinya merupakan worm yang relatif ramah dan biasa-biasa saja. Namun, daya serangnya (penyebarannya) dan kecepatan duplikasinya (setiap 8,5 detik terjadi replikasi) benar-benar mampu mengguncang dunia. Dalam waktu 10 menit sejak kemunculannya, ia mampu menginfeksi 75.000 komputer. worm ini mengakibatkan kerusakan yang signifikan pada dunia bisnis, diantaranya adalah melumpuhnya mesin-mesin cash milik bank sehingga tidak bisa online dan tertundanya beberapa penerbangan yang pengurusan tiketnya dikerjakan oleh komputer yang telah terinfeksi.

Dan ternyata, Sobig juga worm. worm ini tercatat sebagai 'cacing' yang disukai oleh para spammer. Mengapa ? Karena Sobig dapat menjadikan setiap komputer yang ia jangkiti menjadi titik relay (tongkat estafet) bagi para spammer untuk menyebarkan replika Sobig secara massal kepada korban yang akan dituju.

2004 : MyDoom, Netsky, Bagle, dan Sasser ... whoever win, we are lose !

MyDoom alias Novarg dikenal sebagai virus yang menyebar paling cepat dalam sejarah dunia virus, mengungguli Melissa yang populer pada tahun 1999. virus ini menyebar melalui e-mail dan software file sharing. Ia memikat calon korban dengan cara memberitahukan kepada mereka bahwa salah satu e-mail yang telah mereka kirimkan sebelumnya telah gagal terkirim. Hal ini merupakan sebuah trik cerdas nan sederhana untuk mengelabui para korban.

Motif sesungguhnya dari virus ini adalah sebagai alat bagi para hacker untuk melancarkan serangan DoS (Denial of Service) kepada server komputer SCO Inc. (Santa Cruz Operation), dan berhasil. Setelah serangan DoS terjadi, yaitu pada tanggal 1 September 2004, situs perusahaan yang dibenci kalangan open source ini sempat offline beberapa hari. Saking seriusnya, SCO rela memberikan reward sebesar \$ 250.000,00 bagi mereka yang mampu memberitahukan siapa dibalik pembuatan virus ini.

Sven Jaschan, remaja sekolah menengah asal Jerman mengaku menulis Sasser. worm ini tidak menyebabkan kerusakan teknis pada komputer, hanya saja ia mampu mengakibatkan beberapa komputer yang diinfeksi menjadi lambat dan me-reboot dirinya sendiri tanpa dikehendaki oleh sang user. Tercatat, beberapa perusahaan besar menjadi korban worm ini. Seperti maskapai penerbangan kebanggaan Inggris, British Airways, Britain's Coast Guard, RailCorp Australia, dan bahkan dua rumah sakit di Swedia gagal meng-online-kan 5000 komputer mereka karena worm ini. Ketika ditanya oleh polisi Jerman mengenai motif dibalik pembuatan worm ini, Jaschan menjawab bahwa Sasser ditulis untuk menghadapi para Spammer yang berada di balik pembuatan Baggle dan MyDoom.

Netsky ditulis oleh Jaschan untuk menghadapi serangan spammer yang menggunakan Bagle dan MyDoom. Jadi ketika Bagle dan myDoom sedang mengeset aksinya untuk menjadikan setiap komputer yang diinfeksi sebagai tempat pembuangan bulk mail, Netsky akan melakukan sebaliknya.

1.7 Mobile Technology, Sasaran Virus Masa Depan

1.7.1. Telepon Seluler

Telepon seluler dapat terinfeksi oleh virus worm yang menyebarkan dirinya melalui jaringan telepon seluler, meskipun sampai tulisan ini diturunkan belum begitu banyak risiko yang ditimbulkannya. Pada tahun 2004, worm pada telepon seluler pertama kali ditemukan. Worm Cabir-A ini menyerang telepon seluler yang menggunakan sistem operasi Symbian. Worm ini menyebarkan dirinya sendiri dan nampak seperti game dengan format file SIS. Jika Anda menjalankan file ini, maka akan muncul pesan pada layar dan worm akan jalan setiap kali Anda menyalakan telepon seluler.

Cabir-A akan mencari telepon seluler lain di sekitarnya dengan memanfaatkan teknologi Bluetooth dan akan mengirimkan dirinya sendiri ke telepon seluler tersebut. Worm ini membuktikan kepada publik bahwa infeksi virus pada telepon seluler sudah terjadi dan wajib diwaspadai. Ada juga virus konvensional yang mengirimkan pesan ke telepon seluler. Contohnya Timo-A, yang menggunakan modem komputer untuk mengirimkan SMS ke nomor telepon seluler tertentu.

Tetapi virus ini tidak sampai menginfeksi atau merusak telepon seluler. Sampai tulisan ini dipublikasikan, memang virus pada telepon seluler belumlah begitu banyak. Ini disebabkan karena banyaknya sistem operasi yang ada dan juga karena karakteristik baik software maupun device yang cepat berubah.

1.7.2. Palmtop atau PDA

Palmtop, handheld atau PDA membuka peluang bagi virus untuk diserang, walaupun saat ini belum banyak ditemukan gangguan yang ada. PDA atau palmtop berjalan dengan suatu sistem operasi seperti Palm, Symbian, Linux atau PocketPC. Ini bisa dimanfaatkan oleh worm untuk diserang tetapi saat ini risiko tersebut masih belum begitu terlihat. Para pembuat virus tampaknya lebih tertarik mentargetkan sistem komputer desktop untuk virus yang dibuatnya. Ini disebabkan karena pengguna komputer desktop saat ini lebih populer dan juga penyebaran virus bisa sangat cepat dengan adanya e-mail dan internet.

Mungkin bahaya pada palmtop saat ini adalah mereka digunakan sebagai carrier bagi worm. Begitu Anda melakukan sinkronisasi palmtop atau PDA Anda dengan komputer maka worm tadi akan menyebar ke PC Anda dan melakukan aksinya. Untuk mencegah hal ini maka gunakan selalu anti-virus yang definisi virusnya selalu terupdate.

1.7.3. SmartPhone

Bila kita mencoba melihat jauh ke depan ke dalam gelombang kemajuan TI (Teknologi Informasi) maka akan semakin jelaslah bahwa komputer itu tidak hanya desktop atau laptop yang sudah umum kita temui. TabletPC, Ponsel, atau PDA yang terlihat kompak dengan genggam tangan pun sejatinya sudah pantas jika disebut sebagai komputer. Khususnya untuk produk-produk keluaran terbaru yang telah diinjeksi dengan varian sistem operasi macam Symbian OS atau Ms Windows Mobile untuk ponsel, atau Palm OS dan Ms Windows PocketPC untuk PDA.

Berdasarkan fakta di atas, kita dapat mengambil kesimpulan bahwa suatu hari gadget-gadget tersebut pasti akan dijangkiti oleh virus. Dan terbukti, benar! Untuk SmartPhone, setelah Cabir hadir dan menyebar dengan bantuan

Bluetooth yang terinfeksi, menyusullah dua malware terbaru, yaitu Mosquito dan Skull Trojan. Mosquito merupakan sebuah game yang bekerja di Symbian, lucunya selain dapat menghibur penggunanya ia juga secara diam-diam mengirimkan pesan (sms) ke nomor-nomor tertentu yang bersifat layanan (service) berbayar, sehingga menyebabkan lenyapnya pulsa ponsel tersebut.

Lain halnya dengan Skull Trojan, program shareware yang di download dari salah satu situs internet ini dapat mengakibatkan tidak berfungsinya aplikasi-aplikasi yang berjalan pada smartphone anda plus jejak yang manis dengan mengganti icon-icon program aplikasi tersebut dengan icon-icon bergambar tengkorak. Satu-satunya kebaikan yang ditinggalkan oleh Trojan ini adalah ketika ia masih mengizinkan anda untuk berhallo-hallo ria, tapi itu saja, cukup itu saja.

Gambaran di atas benar-benar tidak bisa dianggap remeh. Terlebih di era mobile seperti ini, di mana kelancaran suatu aktivitas sudah menjadi sangat tergantung dengan keberadaan gadget tersebut. Sebut saja mobile banking, aktivitas yang mengandung uang secara lambat laun akan dimanfaatkan oleh para pembuat virus untuk menciptakan varian yang tidak hanya merusak sistem ponsel tersebut tetapi juga mampu mengirimkan data-data tertentu yang sifatnya rahasia kepada sang pembuat virus. Nomor telepon dalam phonebook misalnya.

1.7.4. Teknologi Bluetooth

Bluetooth merupakan teknologi untuk piranti nirkabel yang memungkinkan komputer, telepon seluler, PDA dan lain sebagainya untuk saling terhubung dalam suatu jarak tertentu. Bluetooth mampu untuk mengadakan koneksi antar peralatan-peralatan tersebut secara transparan. Saat ini Bluetooth juga sudah dieksploitasi oleh worm pada telepon seluler. Bluetooth digunakan sebagai media untuk penyebaran worm ke telepon seluler yang lain. Teknologi yang berbasis Bluetooth, seperti Jini, juga mampu melakukan kontrol jarak jauh terhadap suatu service.

Bluetooth dan Jini didesain bahwa hanya kode yang valid dan terpercaya saja yang mampu untuk membawa operasi-operasi yang sifatnya sensitif. Tetapi teknologi-teknologi tersebut juga membuka peluang bagi kode-

kode jahat yang mengganggu jalannya service tersebut. Anda dapat mencegah risiko Bluetooth ini dengan cara mematikan setting Bluetooth "visible to others" pada telepon seluler Anda

1.8 Mencegah virus

Ada beberapa hal yang bisa dilakukan untuk mencegah virus, berikut ini akan disajikan hal-hal tersebut.

- Membuat orang paham terhadap risiko virus,
Katakan kepada semua orang bahwa mereka selalu dalam risiko ketika membuka e-mail, membuka attachment e-mail, download file dari suatu situs atau saling bertukar disket. Mereka harus mengerti bahwa bahaya virus ada dimana-mana dan berhati-hatilah.
- Install program anti-virus dan update-lah secara reguler,
Program anti-virus dapat mendeteksi dan terkadang mampu untuk membasmi virus. Jika program tersebut menawarkan on-access scanner, segera saja gunakan fasilitas tersebut.
- Selalu gunakan software patch untuk menutup lubang security,
Selalu monitor perkembangan patch untuk sistem operasi yang Anda gunakan. Jika ada yang baru segera di-download dan jalankan agar menutup lubang security yang ada pada komputer Anda. Ini akan membuat virus sedikit sulit untuk menyebar.
- Gunakan firewall,
Sebuah firewall mampu untuk mencegah akses ilegal ke sistem komputer atau jaringan Anda. Ini juga bisa mencegah penyebaran virus secara cepat ke dalam jaringan.
- Selalu backup secara reguler data Anda,
Selalu buatlah backup untuk semua data yang ada pada komputer Anda. Pilihlah data dan program yang Anda anggap penting dan lakukan backup secara reguler. Jika sewaktu-waktu komputer Anda terinfeksi virus maka Anda masih bisa melakukan restore dengan data dan program yang bersih.

BAB II PROGRAM ANTIVIRUS

2.1 Definisi Antivirus

Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mendeteksi dan menghapus virus komputer dari sistem komputer. Disebut juga Virus Protection Software. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan). Sebagian besar antivirus bekerja dengan beberapa metode seperti di bawah ini:

Pendeteksian dengan menggunakan basis data *virus signature* (*virus signature database*): Cara kerja antivirus ini merupakan pendekatan yang banyak digunakan oleh antivirus tradisional, yang mencari tanda-tanda dari keberadaan dari virus dengan menggunakan sebagian kecil dari kode virus yang telah dianalisis oleh vendor antivirus, dan telah dikatalogisasi sesuai dengan jenisnya, ukurannya, daya hancurnya dan beberapa kategori lainnya. Cara ini terbilang cepat dan dapat diandalkan untuk mendeteksi virus-virus yang telah dianalisis oleh vendor antivirus, tapi tidak dapat mendeteksi virus yang baru hingga basis data virus signature yang baru diinstalasikan ke dalam sistem. Basis data virus signature ini dapat diperoleh dari vendor antivirus dan umumnya dapat diperoleh secara gratis melalui download atau melalui berlangganan (*subscription*).

Pendeteksian dengan melihat cara bagaimana virus bekerja: Cara kerja antivirus seperti ini merupakan pendekatan yang baru yang dipinjam dari teknologi yang diterapkan dalam Intrusion Detection System (IDS). Cara ini sering disebut juga sebagai *Behavior-blocking detection*. Cara ini menggunakan policy (kebijakan) yang harus diterapkan untuk mendeteksi keberadaan sebuah virus. Jika ada kelakuan perangkat lunak yang "tidak wajar" menurut policy yang diterapkan, seperti halnya perangkat lunak yang mencoba untuk mengakses address book untuk mengirimkan e-mail secara massal terhadap daftar e-mail yang berada di dalam address book tersebut (cara ini sering digunakan oleh virus untuk menularkan virus melalui e-mail), maka antivirus akan menghentikan proses yang dilakukan oleh perangkat lunak tersebut.

Antivirus juga dapat mengisolasi kode-kode yang dicurigai sebagai virus hingga administrator menentukan apa yang akan dilakukan selanjutnya. Keuntungan dari cara ini adalah antivirus dapat mendeteksi adanya virus-virus baru yang belum dikenali oleh basis data *virus signature*. Kekurangannya, jelas karena antivirus memantau cara kerja perangkat lunak secara keseluruhan (bukan memantau berkas), maka seringkali antivirus membuat alarm palsu atau "*False Alarm*" (jika konfigurasi antivirus terlalu "keras"), atau bahkan mengizinkan virus untuk berkembangbiak di dalam sistem (jika konfigurasi antivirus terlalu "lunak"), terjadi false positive. Beberapa produsen menyebut teknik ini sebagai *heuristic scanning*.

Antivirus yang menggunakan *behavior-blocking detection* ini masih sedikit jumlahnya, tapi di masa yang akan datang, kemungkinan besar semua antivirus akan menggunakan cara ini. Beberapa antivirus juga menggunakan dua metode di atas secara sekaligus.

Program antivirus mampu mendeteksi virus dan mencegah akses ke dokumen yang terinfeksi dan juga mampu menghilangkan infeksi yang terjadi. Program pemindai virus merupakan jenis yang paling populer dalam dunia antivirus, tetapi program-program seperti ini harus sering diperbarui agar mampu mengenali virus-virus baru. Secara umum ada dua jenis program antivirus, yaitu *on-access* dan *on-demand scanner*. Banyak perusahaan yang menawarkan gabungan dua jenis program tersebut dalam satu paket.

- ***On-access scanner*** akan selalu aktif dalam sistem komputer selama Anda menggunakannya. Pemindai jenis ini akan secara otomatis memeriksa dokumen-dokumen yang Anda akses dan dapat mencegah Anda menggunakan dokumen yang sudah terinfeksi oleh virus komputer.
- ***On-demand scanner*** membiarkan Anda yang akan memulai aktivitas pemindaian terhadap semua dokumen di komputer Anda. Ini juga bisa Anda atur agar bisa dilakukan secara periodik dengan menggunakan penjadwal.

Ada juga jenis anti-virus yang menerapkan pemindaian secara *heuristic*. Cara ini memungkinkan pemindai mendeteksi virus, baik yang sudah diketahui atau belum, dengan menggunakan aturan-aturan yang umum yang menjadi indikator adanya suatu virus. Ini sangat berguna untuk mendeteksi virus-virus jenis baru atau yang belum terdeteksi sebelumnya. Jenis *heuristic scanner* ini tidak perlu sering diupdate tetapi efek sampingnya terkadang bisa menimbulkan

kesalahan deteksi, di mana seharusnya itu dokumen atau program normal, tetapi dideteksi dan dianggap sebagai suatu virus.

2.2 Perkembangan Program Antivirus

1. Generasi pertama : “scanner sederhana“.

Antivirus menscan program untuk menemukan signature virus. Teknis ini terbatas untuk deteksi virus-virus yang telah dikenal.

2. Generasi kedua : “scanner yang pintar” (*heuristic scanner*).

Antivirus menggunakan aturan-aturan pintar (*heuristic rules*) untuk mencari kemungkinan infeksi virus.

3. Generasi ketiga : jebakan-jebakan aktivitas (*activity trap*).

Program antivirus merupakan program yang menetap di memori (*memory resident program*). Program ini mengidentifikasi virus melalui aksi- aksinya bukan dari struktur program yang diinfeksi.

4. Generasi keempat : proteksi penuh (*full featured protection*).

Antivirus generasi ini menggunakan beragam teknik antivirus secara bersamaan. Teknik-teknik ini meliputi scanning dan jebakan-jebakan aktivitas.

2.3 Antivirus untuk Smartphone

Pada kuartal 4 (Q4) tahun 2004 kemarin, Nokia mulai melengkapi produknya dengan dukungan antivirus dari vendor besar, yaitu F-Secure. Adapun tipe yang dimaksud adalah Nokia 6670 dan Nokia 7710. Sementara F-Secure sendiri dengan bangga menyatakan bahwa antivirus mereka dirancang untuk dapat bekerja secara real-time dan otomatis melalui mekanisme sms yang telah dipatenkan. Selain Nokia, layanan antivirus dari F-Secure juga digunakan oleh Elisa, salah satu operator seluler yang menawarkan jasa antivirusnya melalui jaringan nirkabel kepada pelanggannya.

Daftar Pustaka

- <http://www.wikimu.com/News/displaynews.aspx?id=685>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.33)
- <http://www.wikimu.com/News/displaynews.aspx?id=686>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.22)
- <http://www.wikimu.com/News/displaynews.aspx?id=728>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.21)
- <http://www.wikimu.com/News/displaynews.aspx?id=800>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.25)
- <http://www.wikimu.com/News/displaynews.aspx?id=825>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.40)
- <http://www.wikimu.com/News/displaynews.aspx?id=803>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.10)
- <http://id.wikipedia.org>
(Diakses pada tanggal 27 Oktober 2008 pukul 10.35)