BAB 02

Virus di Warnet

Masalah malware, virus, dan teman-temannya adalah masalah klasik yang layak diperhatikan oleh pengguna warnet. Warnet adalah tempat umum yang digunakan oleh banyak orang, sehingga kemungkinan tertular virus dari warnet cukup besar. Sebenarnya tentu kita patut waspada bukan hanya untuk warnet saja, karena banyak juga tempat lain yang juga perlu diperhatikan, seperti studio foto, rental komputer, dan sebagainya. Jika Anda sering menggunakan komputer umum, sebaiknya kemungkinan serangan virus perlu diwaspadai.

Sistem serta program yang ada di warnet umumnya cukup terlindungi dari serangan virus, karena kebanyakan warnet diproteksi oleh program semacam DeepFreeze, Returnil, Shadow Defender, Clean Slate, dan lain sebagainya. Kegunaan program tersebut adalah untuk mengembalikan kondisi drive –tempat sistem operasi dan instalasi program– kembali seperti semula ketika komputer di-restart.

Jadi, apa pun gangguan yang terjadi, entah itu serangan virus, keusilan pengguna warnet mengganti-ganti setting komputer/internet, dan sebagainya tidak terlalu menjadi masalah, karena begitu komputer di-

restart maka kondisi program-program dan setting kembali seperti sebelumnya. Dari sisi ini, sebenarnya kita bisa melihat bahwa warnet yang memakai program semacam DeepFreeze, Returnil dan sejenisnya, cukup aman dari serangan virus aktif.

Memang cukup jarang dijumpai warnet yang begitu komputer dinyalakan, ternyata ada virus aktif (hidup) di komputer warnet tersebut. Tetapi walaupun jarang, memang bukan berarti tidak ada. Penulis pernah juga menjumpai virus di beberapa warnet, bahkan antivirusnya terus-terusan mengeluarkan pesan bahwa ada virus di komputer tersebut.

Meskipun jarang, memang ada juga admin warnet yang tidak memasang program proteksi, mungkin alasannya program bentrok dan sejenisnya, atau lebih parah lagi virus masuk duluan secara tidak sengaja saat admin menginstal program sebelum DeepFreeze diaktifkan tanpa dia sadari. Mungkin admin menginstal program tertentu yang bermasalah tanpa dia sadari. Bisa jadi warnet tertentu menginstal program bajakan, file cracknya kemudian dideteksi sebagai malware oleh antivirus terbaru. Ada juga program yang tadinya dianggap aman kemudian terdeteksi sebagai malware ketika antivirusnya ter-update.

Tentu pesan peringatan adanya virus/malware akan sangat mengganggu dan malahan bisa membuat ngeri pengguna warnet tersebut. Penulis rasa tidak ada pengunjung warnet yang senang mendapat oleh-oleh file berbahaya di USB Flash Disk, yang berpotensi merusak/mencuri data di komputer pribadinya.

Walaupun virus aktif lebih jarang dijumpai di warnet, pengguna warnet juga mesti waspada dengan file virus (nonaktif) yang mungkin masih ada di harddisk warnet. Sebagian warnet mengizinkan penyimpanan data di harddisk. Jika Anda secara sengaja/tidak sengaja mengakses file yang bervirus, maka tentu virus yang tadinya tidak aktif akan menjadi aktif.

Anda juga sangat mungkin mendapatkan virus/malware dari internet jika antivirus di warnet tidak di-update. Karena sudah merasa terlindungi dengan program semacam DeepFreeze, sangat mungkin antivirus di warnet jarang di-update, atau bisa jadi update otomatis dari program antivirus justru terhapus oleh DeepFreeze ketika komputer di-restart. Beberapa warnet mengganti Deepfreeze dengan Shadow Defender untuk mengatasi masalah update ini, tetapi ada juga warnet yang tidak terlalu peduli mengenai update Antivirus. Malah ada juga warnet yang tidak menginstal antivirus sama sekali.

Berkaitan dengan beragam kondisi di atas, berikut ini akan penulis uraikan beberapa tip terkait masalah virus di warnet.

2.1 Memakai Antivirus Portabel

Memakai antivirus portabel sebenarnya tidak terlalu ideal dibandingkan memakai antivirus yang terinstal. Salah satu alasannya adalah biasanya antivirus portabel hanya berfungsi sebagai *Scanner*, jarang memiliki fitur *Real Time Protector*. Tetapi seperti kata pepatah "Tak ada rotan akar pun jadi", jika kebetulan warnet yang Anda pakai tidak menginstal antivirus, ya apa boleh buat. Memakai antivirus portabel bisa dijadikan pilihan.

Menginstal sendiri antivirus biasa (non-portabel) di warnet mungkin lebih merepotkan, mengingat ukurannya yang sering kali lebih besar. Kadang kala instalasi program dibatasi di warnet. Juga kadang kala setelah menginstal, komputer butuh di-restart, padahal dalam kondisi terproteksi DeepFreeze. Jadinya me-restart komputer sama artinya membuang instalasi itu sendiri. Kesimpulannya, memakai program portabel mungkin lebih masuk akal mengingat kemungkinan kondisi tersebut.

Jika sering memakai komputer umum, termasuk warnet, ada baiknya Anda mempersiapkan antivirus portabel yang bisa Anda bawa dan Anda jalankan di USB Flash Disk. Ini cukup membantu apabila komputer yang Anda pakai ternyata tidak memiliki antivirus. Ada banyak antivirus portabel yang bisa Anda pilih, seperti Clam Win, Naevius, Rizone, MxOne, dan sebagainya. Pada buku ini, antivirus portabel yang dibahas adalah Clam Win, karena gratis, berukuran kecil, dan cukup ringan.

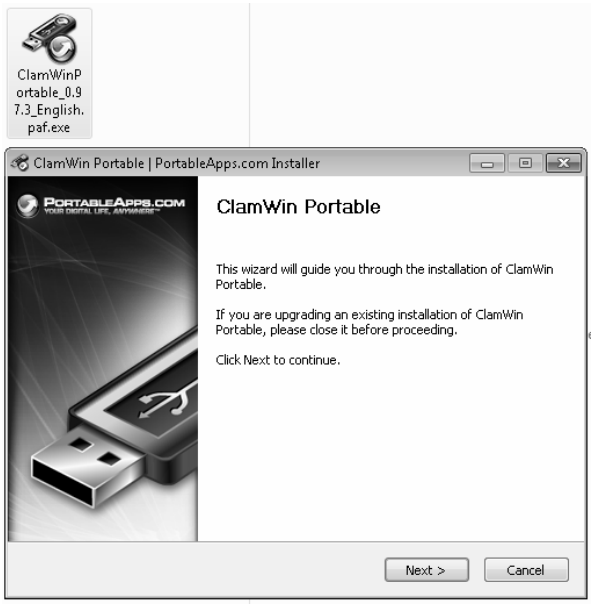
Clam Win bisa Anda download di alamat: http://www.clamwin.com/content/view/18/46/ atau di alamat: http://portableapps.com/apps/utilities/clamwin_portable.

Gambar 2.1 Download Clamwin

Jika Anda memakai komputer warnet, tentu Anda bisa men-download program tersebut di warnet. Anda juga bisa mendapatkannya di Bonus CD buku ini.

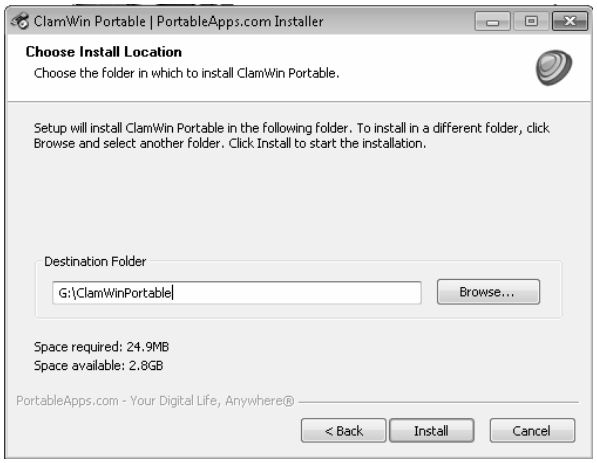
Anda bisa mengekstrak Clam Win langsung di USB Flash Disk. Bisa juga mengekstrak dulu di komputer, baru kemudian Anda salin ke USB Flash Disk. Anggap saja kita akan langsung ekstrak ke Flash Disk.

1. Jalankan program installer yang sudah Anda download. Pastikan sebelumnya sudah ada Flash Disk terpasang di port USB komputer Anda. Klik **Next**.



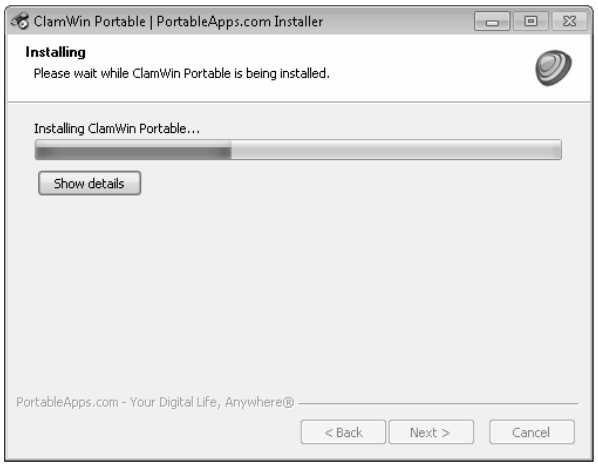
Gambar 2.2 ClamWin Installer

2. Pada **Destination Folder**, klik **Browse** dan pilih drive tempat Anda mencolokkan Flash Disk Anda. Dalam buku ini, drive **G** adalah drive Flash Disk di komputer penulis.



Gambar 2.3 Folder tujuan instalasi di flash disk

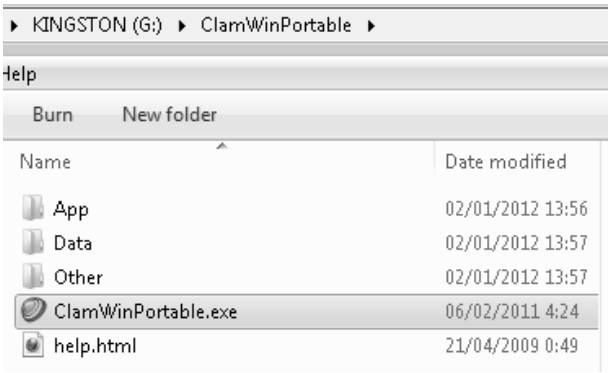
3. Tekan tombol **Install**.



Gambar 2.4 Instalasi ClamWin berlangsung

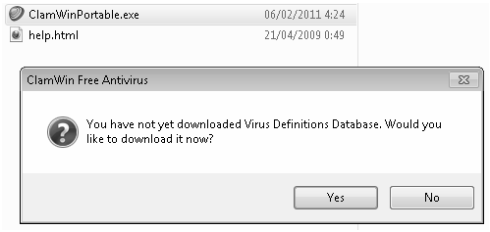
4. Tunggu instalasi sampai selesai, lalu klik tombol **Finish**.

5. Jalankan file **ClamWinPortable.exe** di Flash Disk Anda. Lokasi file tersebut tergantung dari **Destination Folder** yang Anda pilih tadi.



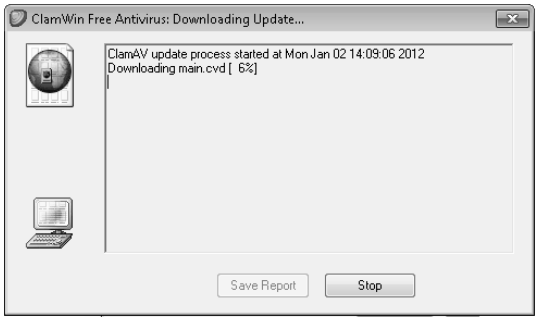
Gambar 2.5 Menjalankan ClamWin

6. Jika ada pertanyaan mengenai download **Virus Definitions Database**, jawab saja dengan menekan tombol **Yes**.



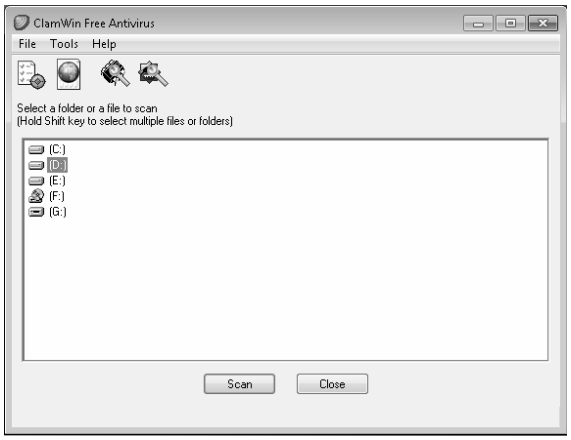
Gambar 2.6 Tawaran update database

7. Tunggu proses update sampai selesai. Setelah update selesai, akan ditampilkan program ClamWin.



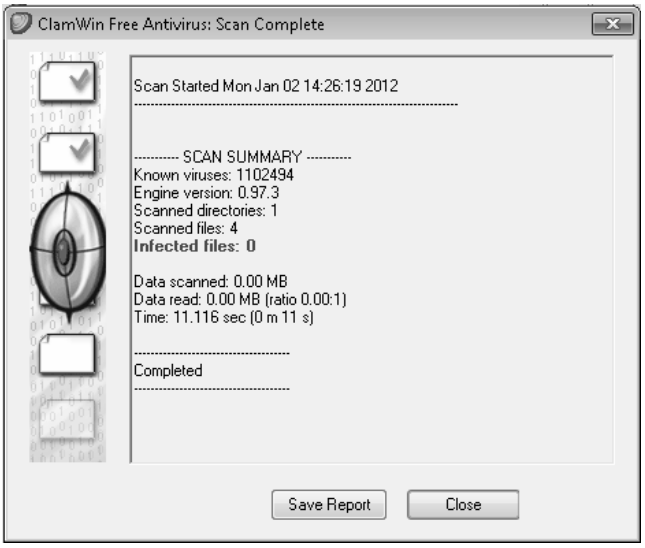
Gambar 2.7 Proses update

8. Sekarang Anda bisa melakukan scan virus.



Gambar 2.8 Scan drive yang Anda inginkan

9. Anda bisa memilih file, folder, atau drive untuk di-scan. Setelah file/folder/drive Anda pilih, tekan saja tombol **Scan**.



Gambar 2.9 Hasil scan

Sekarang, Anda bisa memastikan file yang sudah Anda download atau file yang ada di harddisk warnet cukup aman, sebelum Anda menyimpannya di USB Flash Disk.

Untuk perlindungan lebih, baik juga jika Flash Disk berisi program antivirus dan Flash Disk berisi data dibedakan. Anda copy dulu folder program ClamWin ke harddisk warnet, lalu Anda jalankan. Untuk menyimpan data, lebih baik jika Anda memakai Flash Disk yang lain.

Solusi lain, Anda bisa memakai program pelindung USB Flash Disk yang di dalamnya Anda isi dengan antivirus. Anda bisa juga mencoba antivirus lokal seperti Smadav sebagai alternatif menginstal antivirus luar yang biasanya berukuran lebih besar. Tentu Anda juga bisa mencoba aneka antivirus portabel yang lain. Ada banyak antivirus portabel di internet, misalnya saja di http://www.softpedia.com/hubs/Portable-Antivirus.

2.2 Men-scan File dengan Puluhan Antivirus

Jika kita berada di warnet, kita ingin mengecek keamanan file hasil download atau file yang kita miliki, apakah mengandung malware atau aman. Kita bisa melakukannya cukup mudah dengan Multiple Antivirus Online.

Kelebihan cara ini adalah kita tidak perlu memikirkan apakah di komputer yang kita pakai terinstal antivirus atau tidak, serta apakah update antivirusnya cukup baru atau tidak, karena pengecekan dilakukan di server perusahaan antivirus atau server penyedia layanan multiple antivirus online. File yang kita cek, akan diperiksa dengan belasan bahkan puluhan Antivirus terkemuka dengan update terbaru.

Kekurangannya adalah ukuran dan jumlah file yang bisa diperiksa lebih terbatas. Ini karena proses upload dan pemeriksaan tentu membutuhkan waktu lebih lama ketimbang pengecekan memakai antivirus yang terinstal di komputer.

Berikut ini sejumlah situs internet yang menyediakan Multiple Antivirus Scanner:

- http://vscan.novirusthanks.org/
- http://www.virustotal.com/
- http://www.virscan.org/
- http://virusscan.jotti.org/
- http://www.viruschief.com
- http://www.filterbit.com/
- http://www.garyshood.com/virus/
- http://www.metascan-online.com/

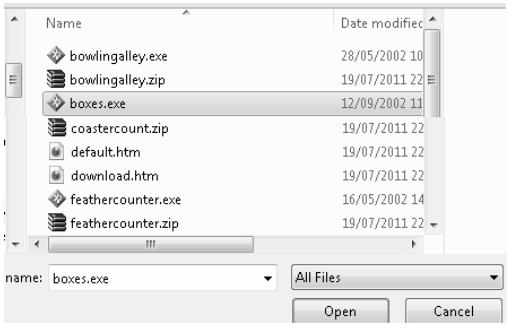
Bagaimana cara memakai situs penyedia layanan multiple antivirus tersebut? Caranya cukup mudah. Kita tinggal upload file yang ingin kita periksa ke penyedia layanan. Kita tunggu beberapa saat, maka laporan akan diberikan. Bisa juga kita isikan alamat email lalu laporan akan dikirimkan ke email kita.

Berikut salah satu contoh pemakaian multiple antivirus online. Pada contoh ini penulis memakai situs http://vscan.novirusthanks.org/. Langkah-Langkahnya sebagai berikut:

1. Buka situs http://vscan.novirusthanks.org/ via browser yang ada di komputer Anda.

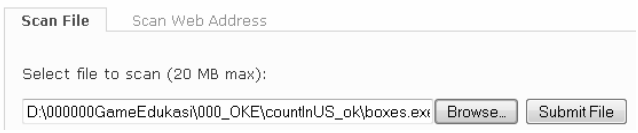
Gambar 2.10 Situs http://vscan.novirusthanks.org/

2. Klik tombol **Browse**. Pilih file di komputer yang ingin Anda periksa. Klik tombol **Open** setelah file terpilih.



Gambar 2.11 Upload file

3. Klik tombol **Submit File**.



Gambar 2.12 Submit file

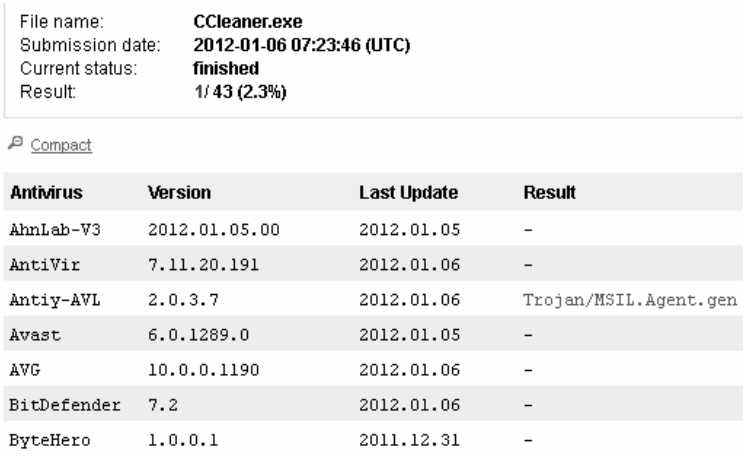
4. Kita harus menunggu beberapa saat sampai file kita terkirim dan dicek. Lamanya proses ini tergantung dari ukuran file, kecepatan internet, serta banyaknya antrian yang mungkin ada. Berikut ini salah satu contoh laporan hasil pemeriksaan. Ternyata file game yang penulis upload bebas dari virus menurut pemeriksaan dari website tersebut, **Status**: **Clean**.

Gambar 2.13 Laporan hasil scan

Sejumlah antivirus yang melakukan tugas pemeriksaan di situs http://vscan.novirusthanks.org/, antara lain Avast, Avira, Antivir, ClamAV, Comodo, Emsisoft, F-Prot, Ikarus, dan Trend Micro.

Di antara sekian website penyedia scan virus dengan multiple antivirus online, salah satu website yang paling menonjol lainnya adalah virustotal.com.

Website ini menyediakan lebih dari 40 Antivirus yang bekerja bersama men-scan file Anda. Cara menggunakannya kurang lebih sama, Anda meng-upload file yang ingin Anda periksa ke website mereka (Virustotal.com), lalu menunggu laporan diberikan. Berikut ini contoh laporan yang diberikan oleh virustotal.com terhadap file yang penulis upload.



File name: **CCleaner.exe**
Submission date: **2012-01-06 07:23:46 (UTC)**
Current status: **finished**
Result: **1 / 43 (2.3%)**

Compact

Antivirus	Version	Last Update	Result
AhnLab-V3	2012.01.05.00	2012.01.05	-
AntiVir	7.11.20.191	2012.01.06	-
Antiy-AVL	2.0.3.7	2012.01.06	Trojan/MSIL.Agent.gen
Avast	6.0.1289.0	2012.01.05	-
AVG	10.0.0.1190	2012.01.06	-
BitDefender	7.2	2012.01.06	-
ByteHero	1.0.0.1	2011.12.31	-

Gambar 2.14 Laporan hasil scan dari VirusTotal.com

Dari 43 antivirus yang memeriksa file executable yang penulis upload, hanya 1 (satu) antivirus yang menyatakan file tersebut bermasalah. Sedangkan 42 antivirus lainnya menganggap file tersebut baik-baik saja.

Kadang kala antivirus memang bisa melakukan kesalahan. Tidak selalu antivirus berhasil mendeteksi virus. Pada sisi sebaliknya, ada juga program yang sebenarnya baik-baik saja tetapi bisa dianggap berpotensi berbahaya oleh antivirus tertentu. Biasanya karena diperkecil dengan packing tertentu yang mencurigakan antivirus. Pada contoh di atas: Ccleaner adalah program pembersih history yang sebenarnya aman, tetapi dianggap berbahaya oleh salah satu antivirus. Sedangkan 42 antivirus lainnya mengatakan file tersebut aman.

Jika kita menjumpai sejumlah besar antivirus menganggap file tersebut aman, biasanya file tersebut memang aman. Tetapi selain soal keamanan, faktor kenyamanan mungkin perlu kita perhatikan. Jika antivirus yang kita pakai entah di rumah atau di kantor adalah antivirus yang kebetulan menyatakan sebuah program tidak aman (walaupun sebenarnya aman), mungkin kita akan direpotkan oleh peringatan-peringatan yang muncul dari antivirus, ketika kita menjalankan program tersebut.

Solusinya, Anda bisa memakai program lain sejenis, yang tidak membuat antivirus Anda *ke-GeeR-an*. Cara lain, jika memungkinkan, Anda mendaftarkan file yang ingin Anda pakai itu ke dalam daftar pengecualian pengecekan antivirus yang Anda pakai. Ini tergantung dari seberapa penting file tersebut bagi Anda. Apakah ada pengganti yang sejenis atau tidak. Jika antivirus Anda yang bermasalah karena terlalu sering melakukan kesalahan, tentu ada baiknya Anda mempertimbangkan memakai antivirus yang lain.

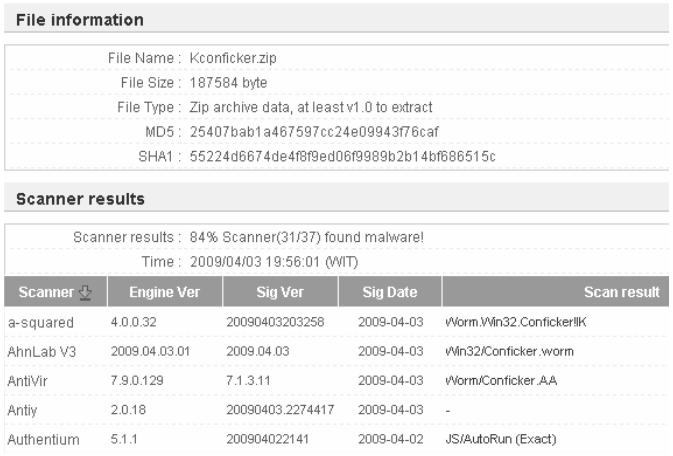
Kemungkinan salah sebenarnya cukup manusiawi dan bisa terjadi pada semua antivirus. Rasanya tidak ada jaminan antivirus manapun yang selalu terbebas dari kemungkinan salah. Salah itu bisa berarti dua pilihan. Pertama menganggap program yang sebenarnya baik dianggap berbahaya, atau sebaliknya program yang sebenarnya berbahaya tetapi dianggap aman.

Pada prinsipnya, saat melakukan pemeriksaan memakai virustotal.com atau situs sejenis, mungkin ada beberapa hal yang sebaiknya Anda perhatikan:

- Pertama, seberapa banyak antivirus yang menyatakan file tersebut aman dibandingkan yang menyatakan tidak aman.

- Kedua, apakah antivirus yang menyatakan aman/tidak aman adalah antivirus yang Anda pakai di rumah/kantor.
- Ketiga, seberapa penting file tersebut, apakah bisa diganti atau tidak, dibandingkan dengan potensi ketidakamanan atau ketidaknyamanan yang mungkin bisa saja terjadi jika Anda memaksa memakai file tersebut mengingat respons antivirus yang Anda pakai.

Walaupun pengecekan virus/malware memakai virustotal.com bisa kita anggap sangat baik, tetapi ada juga gunanya jika kita tahu sejumlah website penyedia antivirus online yang lain. Kadang kala malware melakukan blokir terhadap antivirus dan situs security tertentu yang paling terkenal. Kita bisa menyiasatinya dengan memakai situs lain sejenis (yang tidak terblokir) atau memakai proxy (akan dijelaskan pada bagian lain buku ini).



File information

File Name : Kconficker.zip
File Size : 187584 byte
File Type : Zip archive data, at least v1.0 to extract
MD5 : 25407bab1a467597cc24e09943f76caf
SHA1 : 55224d6674de4f8f9ed06f9989b2b14bf686515c

Scanner results

Scanner results : 84% Scanner(31/37) found malware!
Time : 2009/04/03 19:56:01 (WIT)

Scanner	Engine Ver	Sig Ver	Sig Date	Scan result
a-squared	4.0.0.32	20090403203258	2009-04-03	Worm.Win32.ConfickerIIK
AhnLab V3	2009.04.03.01	2009.04.03	2009-04-03	Win32/Conficker.worm
AntiVir	7.9.0.129	7.1.3.11	2009-04-03	Worm/Conficker.AA
Antiy	2.0.18	20090403.2274417	2009-04-03	-
Authentium	5.1.1	200904022141	2009-04-02	JS/AutoRun (Exact)

Gambar 2.15 Laporan hasil scan dari Worm Conficker

Sebagai contoh kasus, worm Conficker di sebuah komputer melakukan blokir terhadap aneka situs yang dia anggap berpotensi membahayakan eksistensinya, termasuk situs Microsoft, Threat Expert, dan

VirusTotal.com. Tetapi ternyata situs penyedia layanan multiple antivirus online Virscan.org tidak termasuk yang diblokir pada waktu itu. Jadi, kita bisa melakukan pengecekan menggunakan situs tersebut.

Selain meng-upload dengan cara biasa, proses pengecekan file dengan multiple antivirus bisa sedikit dipermudah dengan program X-Ray (http://www.raymond.cc/blog/xray/ atau direct download: http://www.raymond.cc/xray/XRay.zip).

X-Ray membutuhkan Microsoft .NET Framework 4 yang bisa di-download di situs Microsoft:

http://www.microsoft.com/download/en/confirmation.aspx?id=17113
Karena tidak semua warnet terpasang Microsoft NET FrameWork 4, maka dalam kasus pengecekan malware di warnet, mungkin lebih mudah dan praktis jika proses upload dilakukan manual ke situs penyedia Multiple Antivirus Scanner. Jika Anda memakai komputer pribadi di rumah, program X-Ray bisa menjadi alternatif yang cukup menarik untuk mempermudah proses upload file ke situs pengecekan virus online.

2.3 Mengecek Keamanan Link Download

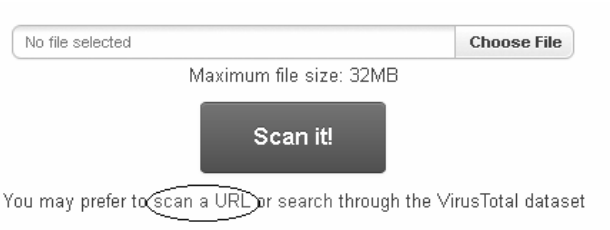
Sebagian situs yang menyediakan layanan scan file dengan multiple antivirus online, biasanya juga menyediakan fitur pengecekan keamanan website. Ini berarti sebelum kita mengunjungi website atau sebelum melakukan download, kita bisa mengecek terlebih dahulu keamanan website atau keamanan file yang akan kita download. Tentu ini lebih menghemat waktu, karena kita tidak perlu men-download file terlebih dahulu ke komputer.

Berikut ini sejumlah situs yang menyediakan pengecekan link website aman atau bervirus/malware.

- https://www.virustotal.com/ (pada bagian scan a URL)
- http://online.drweb.com/?url=1
- http://onlinelinkscan.com/
- http://siteinspector.comodo.com/
- http://www.avg.com.au/resources/web-page-scanner/
- http://linkscanner.explabs.com/linkscanner/default.asp
- http://www.stopbadware.org/home/reportsearch
- http://wepawet.iseclab.org/

Cara menggunakan situs-situs tersebut sangat mudah. Tinggal kita ketikkan atau copy-paste link URL di kotak yang tersedia. Lalu kita tekan tombol **Scan** atau sejenisnya. Berikut ini contohnya:

1. Anggap saja Anda ingin memakai situs virustotal.com. Ketik **virustotal.com** di browser kesukaan Anda, lalu **Enter** atau tekan **Go**.
2. Setelah halaman situs virustotal.com tampil, perhatikan di bawah tombol **Scan it!** ada link biru **scan a URL**. Klik link **Scan a URL** tersebut.



Gambar 2.16 Link scan a URL di situs virustotal.com

3. Selanjutnya ketik atau copy-paste link yang ingin Anda cek keamanannya di kotak **Enter URL**. Lalu tekan tombol **Scan It!**.

Gambar 2.17 Copy-paste masukkan link yang ingin Anda cek lalu klik Scan it!

4. Sesaat kemudian virustotal akan menampilkan hasil pengecekan terhadap link yang Anda inputkan.

Gambar 2.18 Laporan hasil scan URL

Gambar di atas sengaja dipotong untuk menghemat tempat. Di bagian bawahnya masih ada data dari URL Scanner yang lain. Ternyata dari 19 URL Scanner, 18 Scanner mengatakan link tersebut *clean site* atau aman, dan hanya satu yang mengatakan itu *malware site*. Dalam kasus seperti ini, kemungkinan besar link tersebut aman karena perbedaan yang mengatakan aman dan tidak aman sangat besar. 18 dari 19 mengatakan aman. Tetapi tentu menjadi pertimbangan masing-masing orang untuk men-download atau tidak, mengunjungi situs tersebut atau tidak, berdasarkan hasil analisis yang disajikan oleh situs URL Scanner tersebut.

Selain melalui situs yang menyediakan link scanner, pengecekan bisa juga dilakukan dengan add-ons Mozilla Firefox dari DrWeb. Add-ons bisa

di-download di https://addons.mozilla.org/en-US/firefox/addon/drweb-anti-virus-link-checker/. Bisa juga memakai software pengecekan link download dari AVG yang bisa di-download secara gratis di: http://linkscanner.avg.com/. Dalam kasus di warnet, memakai situs online mungkin lebih praktis ketimbang menginstal add-ons atau menginstal program.

Selain memakai scan antivirus, sebuah domain atau subdomain juga bisa dicek reputasinya, misalnya memakai situs:

- http://www.mywot.com/
- http://www.linkextend.com
- http://www.trustedsource.org/
- http://www.siteadvisor.com/sites/

Semakin sebuah situs mendapat reputasi baik di masyarakat internet sedunia, tentu kemungkinan isi situs tersebut aman semakin besar. Pemakaiannya kurang lebih sama. Anda tinggal mengisikan atau meng-copy-paste URL yang ingin Anda cek ke kotak yang tersedia, lalu tekan **Enter**, klik tombol **Go**, atau sejenisnya. Beberapa saat kemudian akan ditampilkan laporan terkait link yang Anda inputkan. Karena ini kaitannya dengan reputasi di mata masyarakat internet, maka ada kemungkinan situs-situs baru belum memiliki data yang bisa ditam-pilkan.

Berikut hasil laporan situs mywot.com terhadap salah satu situs populer di Indonesia, yaitu situs berita detik.com.

Gambar 2.19 Reputasi sebuah situs di mata pengguna internet

2.4 Menganalisis Perilaku Virus dengan Mudah

Dengan bantuan situs semacam Virustotal.com, kita bisa dengan mudah mengecek apakah sebuah file berpotensi membahayakan atau tidak. Tetapi andaikata file tersebut dianggap berbahaya, kita tidak tahu apa sebenarnya yang dilakukan file tersebut sehingga dianggap berbahaya. Virustotal hanya memberikan tanda berbahaya atau tidak, tetapi tidak menunjukkan apa perilaku dari file tersebut.

Bagi sebagian besar orang, pemberitahuan aman atau tidak aman mungkin dirasa cukup. Tetapi bagi sebagian lainnya, mungkin ada rasa penasaran mengapa sebuah file dianggap berbahaya. Apa alasannya?

Untuk menganalisis isi sebuah file program dan bagaimana perilakunya ketika file tersebut dijalankan, diperlukan kemampuan *reverse engineering*. Ini sebenarnya pekerjaan cracker dan pakar-pakar virus untuk melakukan analisis, baik secara langsung dengan membedah kode program maupun tidak langsung dengan melihat perilaku program.

Menganalisis file “mencurigakan” memiliki potensi bahaya yang cukup besar, karena file tersebut sangat mungkin melakukan perusakan terhadap isi komputer kita. Para pakar biasanya melakukan analisis dengan komputer terisolasi atau memakai program khusus yang menciptakan tempat virtual, di mana malware bisa diisolasi, sengaja diaktifkan, dan diperhatikan perilakunya.

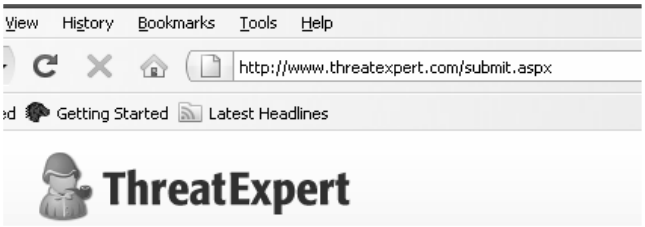
Walaupun demikian, kita yang awam dalam bidang pembedahan dan analisis file bisa saja sekali waktu menjadi “pakar dadakan”, yaitu dengan memanfaatkan aneka situs yang ada di internet.

Berikut ini sejumlah situs yang bisa kita manfaatkan untuk menganalisis perilaku file program yang kita miliki:

- http://www.threatexpert.com/submit.aspx
- http://www.threattrack.com/
- http://camas.comodo.com/cgi-bin/submit
- http://www.norman.com/security_center/security_tools/
- http://anubis.iseclab.org/index.php
- http://www.uploadmalware.com/

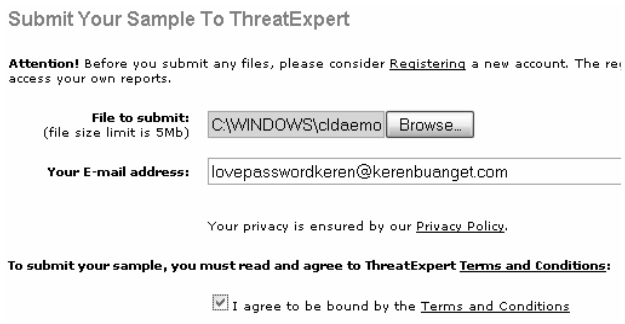
Berikut ini salah satu cara penggunaannya:

1. Silakan masuk ke salah satu situs di atas, pada buku ini anggap saja Anda memilih menggunakan situs threatexpert. Buka situs http://www.threatexpert.com/submit.aspx dengan browser kesukaan Anda.



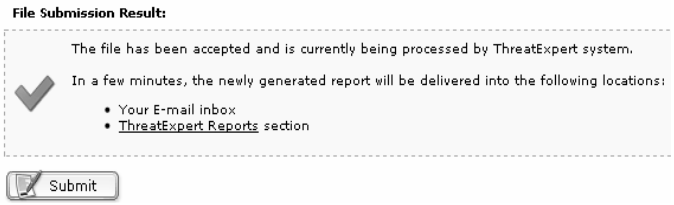
Gambar 2.20 Situs ThreatExpert.com

2. Silakan upload file yang ingin Anda analisis. Isikan alamat email. Centang pada bagian **I agree to be bound by the Terms and Conditions**. Lalu klik tombol **Submit** di bagian bawah.



Gambar 2.21 Kirimkan sampel file

Beberapa saat kemudian akan muncul laporan bahwa file telah diterima, file sedang diproses. Laporan hasil analisis akan dikirimkan ke alamat email Anda dan juga pada ThreatExpert Report.



Gambar 2.22 File telah diterima

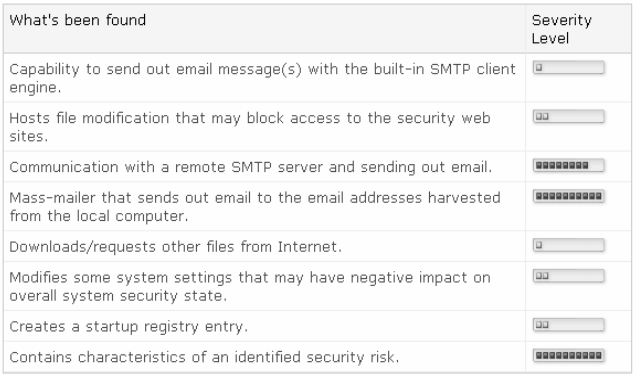
Lalu apa kelebihan situs analisis file dibandingkan dengan virustotal dan situs multiple antivirus scan lainnya?

Kelebihannya adalah karena laporannya jauh lebih lengkap. Tidak sekadar aman atau tidak aman, tetapi juga melaporkan apa saja sebenarnya yang dikerjakan oleh malware atau apa pun file yang kita upload.

Laporan yang diberikan meliputi perubahan apa saja yang terjadi pada file sistem, registry Windows, apakah malware mencoba men-download file atau mengakses file tertentu, dan sebagainya. Laporannya cukup menyeluruh dari berbagai sisi.

Berikut ini contoh laporan yang disajikan Threat Expert terhadap file yang penulis upload.

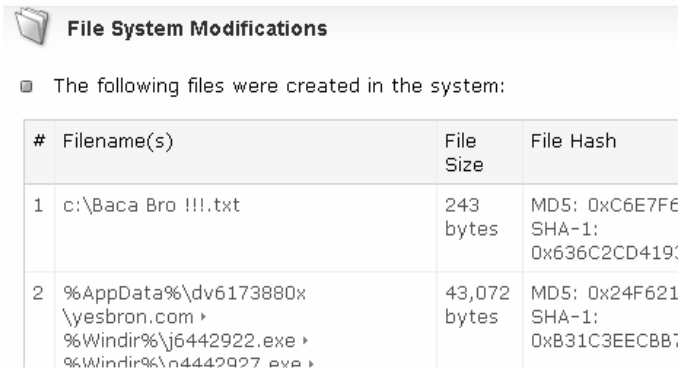
- Contoh laporan umum:



What's been found	Severity Level
Capability to send out email message(s) with the built-in SMTP client engine.	
Hosts file modification that may block access to the security web sites.	
Communication with a remote SMTP server and sending out email.	
Mass-mailer that sends out email to the email addresses harvested from the local computer.	
Downloads/requests other files from Internet.	
Modifies some system settings that may have negative impact on overall system security state.	
Creates a startup registry entry.	
Contains characteristics of an identified security risk.	

Gambar 2.23 Laporan umum hasil analisis Malware

- Contoh laporan analisis file apa saja yang dimodifikasi atau diciptakan oleh worm tersebut:



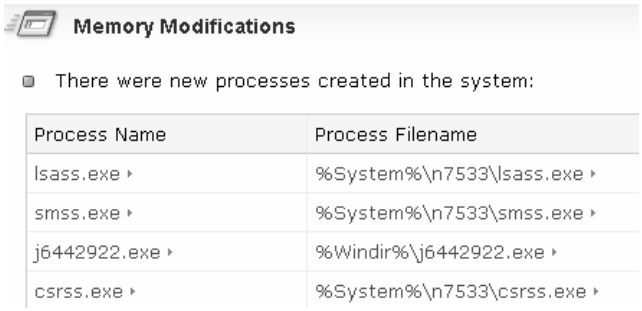
File System Modifications

The following files were created in the system:

#	Filename(s)	File Size	File Hash
1	c:\Baca Bro !!!.txt	243 bytes	MD5: 0xC6E7F6 SHA-1: 0x636C2CD419
2	%AppData%\dv6173880x \yesbron.com ▸ %Windir%\j6442922.exe ▸ %Windir%\n4442927.exe ▸	43,072 bytes	MD5: 0x24F621 SHA-1: 0xB31C3EECBB

Gambar 2.24 Laporan file apa yang dibuat Malware

- Laporan file apa saja yang berjalan di belakang layar atau pada memory:



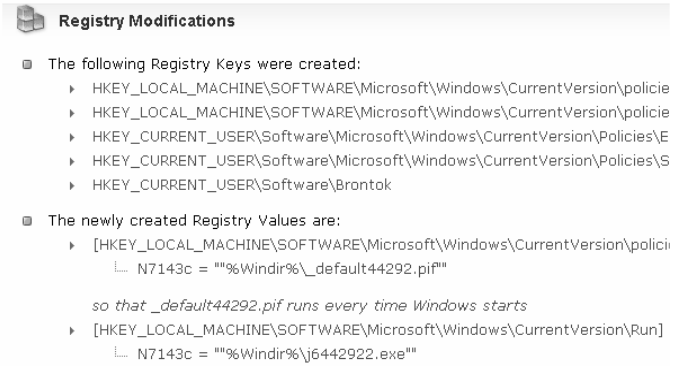
Memory Modifications

There were new processes created in the system:

Process Name	Process Filename
lsass.exe ▸	%System%\n7533\lsass.exe ▸
smss.exe ▸	%System%\n7533\smss.exe ▸
j6442922.exe ▸	%Windir%\j6442922.exe ▸
csrss.exe ▸	%System%\n7533\csrss.exe ▸

Gambar 2.25 Laporan process yang berjalan di belakang layar

- Laporan apa saja bagian dari registry yang diubah atau dibuat oleh worm tersebut:



Gambar 2.26 Laporan perubahan pada registry

Setelah mendapatkan hasil analisis yang begitu lengkap, tentu Anda menjadi lebih tahu tindakan apa yang mungkin dilakukan oleh file tersebut. File yang penulis upload adalah file exe virus/worm brontok yang pernah populer beberapa waktu lalu.

Bagi rekan-rekan yang kebetulan komputernya sedang terinfeksi virus, pengetahuan semacam ini juga bermanfaat untuk melakukan pembasmian virus secara manual. Kita jadi tahu file apa saja yang harus kita bunuh, kita kill prosesnya. Lebih jauh lagi karena kita tahu pasti file apa saja yang dibuat virus, maka kita juga tanpa ragu-ragu bisa menghapus file tertentu karena bisa kita pastikan file tersebut layak dihapus. Kita juga tahu registry yang mesti dihapus atau diperbaiki dengan lebih pasti.

2.5 Mengamati Keberadaan Virus secara Manual

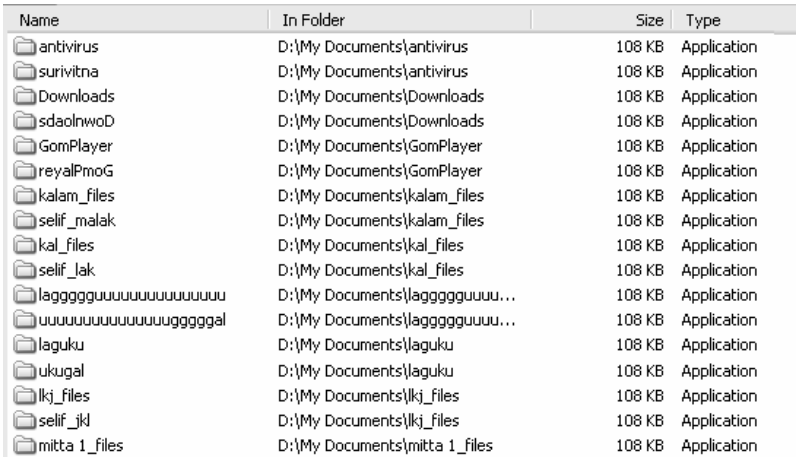
Secanggih apa pun sebuah antivirus, selalu ada kemungkinan antivirus melakukan kesalahan. Bisa saja antivirus menganggap file tertentu membahayakan meskipun sebenarnya aman, bisa juga sebaliknya file yang berbahaya malah dibiarkan begitu saja. Kadang kala pengamatan

secara manual bisa juga membantu menemukan virus/malware yang terlewatkan oleh antivirus. Jika Anda memakai komputer pribadi, kondisi seperti **regedit** mendadak tidak bisa diakses, atau **Show hidden files** di **Folder Options** mendadak tidak berfungsi dan selalu kembali ke setting hidden, bisa jadi semacam pertanda kasar ada malware di komputer Anda.

Masalahnya memang menjadi agak berbeda di warnet, karena sering kali regedit yang terblokir justru bukan pertanda ada virus di komputer tersebut, karena blokir justru dilakukan admin warnet.

Walaupun mengamati jejak virus di warnet kadang kala agak susah karena tidak jelas mana yang hasil kerja virus dan mana yang dilakukan admin, tetapi kadang kala kita bisa juga mendapatkan jejak yang sangat mencolok mata. Bisa saja jejak virus yang sebenarnya mencolok mata itu justru belum terdeteksi oleh antivirus.

Di dalam sebuah warnet yang penulis kunjungi, terdapat program antivirus yang lumayan populer. Penulis cek sejenak antivirus tersebut. Ternyata antivirus yang terpasang tergolong baru, dan sudah di-update pada waktu itu. Anehnya, di folder data harddisk warnet tersebut bertebaran tampilan folder mencurigakan yang kemungkinan besar itu worm atau virus lokal. Mengapa bisa penulis simpulkan demikian? Karena ada ciri umum tertentu seperti file adalah aplikasi (file exe) tetapi ikonnya dibuat berbentuk folder, ukurannya sejenis semua dan berte-baran di banyak folder. Namanya juga dibuat sama dengan nama folder induknya.

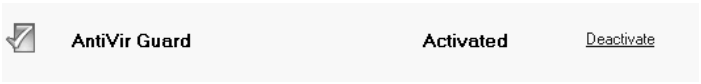


Name	In Folder	Size	Type
antivirus	D:\My Documents\antivirus	108 KB	Application
surivitna	D:\My Documents\antivirus	108 KB	Application
Downloads	D:\My Documents\Downloads	108 KB	Application
sdaolnwoD	D:\My Documents\Downloads	108 KB	Application
GomPlayer	D:\My Documents\GomPlayer	108 KB	Application
reyalPmoG	D:\My Documents\GomPlayer	108 KB	Application
kalam_files	D:\My Documents\kalam_files	108 KB	Application
selif_malak	D:\My Documents\kalam_files	108 KB	Application
kal_files	D:\My Documents\kal_files	108 KB	Application
selif_lak	D:\My Documents\kal_files	108 KB	Application
laggggguuuuuuuuuuuuu	D:\My Documents\laggggguuuu...	108 KB	Application
uuuuuuuuuuuuuuuggggal	D:\My Documents\laggggguuuu...	108 KB	Application
laguku	D:\My Documents\laguku	108 KB	Application
ukugal	D:\My Documents\laguku	108 KB	Application
lkj_files	D:\My Documents\lkj_files	108 KB	Application
selif_jkl	D:\My Documents\lkj_files	108 KB	Application
mitta 1_files	D:\My Documents\mitta 1_files	108 KB	Application

Gambar 2.27 Virus di sebuah warnet

Tanpa memakai tool apa pun, orang yang melihat kondisi ini bisa segera menyimpulkan bahwa file-file tersebut tergolong file yang “tidak beres”.

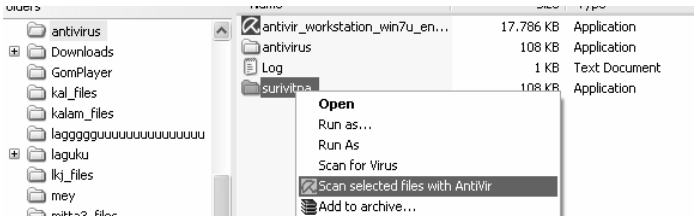
Tetapi antivirus yang terinstal dan sudah di-update ternyata tidak mendeteksi kondisi tersebut. Meskipun penulis membuka folder yang menyimpan file-file “berbahaya” itu, antivirus tetap adem-ayem padahal penulis melihat pada setting-nya, Antivirus Guard dalam kondisi aktif atau *activated*.



Gambar 2.28 Antivirus aktif

Kurang puas dengan situasi ini, penulis mencoba men-scan salah satu file aplikasi dengan ikon berbentuk folder memakai antivirus yang terinstal.

Hasilnya sama seperti dugaan penulis, memang antivirus tersebut gagal mendeteksi: **The scan has finished! Last Detection: No detection**.

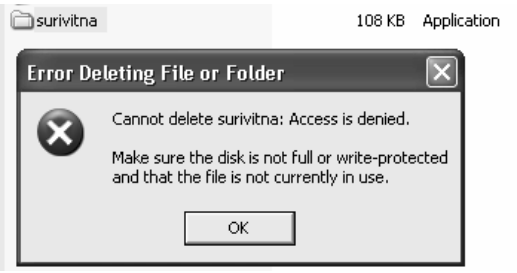


Gambar 2.29 Scan file dengan antivirus yang ada di warnet

Penulis tidak hendak menjelek-jelekkan salah satu perusahaan atau vendor antivirus, yang dalam kasus ini kebetulan gagal mendeteksi worm yang bahkan kelihatan secara kasat mata. Kasus seperti ini adalah sesuatu yang sebenarnya biasa saja. Ini bisa terjadi pada antivirus manapun. Worm, virus, dan teman-temannya selalu berkembang sehingga selalu ada kemungkinan bahwa ada virus tertentu yang gagal dideteksi oleh antivirus meskipun sudah di-update. Bisa juga terjadi sebaliknya, ada file yang sebenarnya biasa saja tetapi justru dianggap berbahaya. Ini kondisi sangat umum yang kadang kala bisa terjadi.

Yang ingin penulis katakan sebenarnya sederhana saja: Biar pun antivirus itu canggih, antivirus juga sangat berguna –tetapi ada kalanya mata seorang pengguna bisa membantu melengkapi kinerja antivirus yang ada. Bukan menggantikan, tetapi melengkapi. Pada contoh ini, pengguna komputer bisa langsung mendeteksi kalau ada file-file yang tidak beres meskipun antivirusnya gagal mendeteksi.

Penulis sempat mencoba menghapus salah satu file, tetapi ternyata gagal. Ini menandakan bahwa virus atau worm di komputer tersebut aktif. Entah karena secara tidak sengaja kena senggol, atau sebelumnya memang sudah aktif, atau virus itu disenggol oleh orang lain sebelum penulis karena komputer pada saat log on billing baru, tidak otomatis di-restart. Ketika penulis memakai komputer tersebut, komputer sudah dalam keadaan menyala dan penulis tinggal memasukkan user name ke program billing.



Gambar 2.30 File tidak bisa dihapus

Dalam kasus berkomputer di warnet, ada beberapa hal yang mungkin bisa kita laksanakan.

Sebagai langkah awal –termasuk bila Anda merasa di komputer ada virus/worm/malware lainnya– ada baiknya jika Anda me-restart komputer entah bagaimana caranya, baik memakai restart dari program billing kalau ada, memakai Start menu Windows, atau bila terpaksa memakai jurus "jari sakti", yaitu tekan tombol **Reset** pada CPU atau tekan tombol **Power**-nya agak lama.

Mengapa ini sebaiknya dilakukan? Alasannya demikian: Komputer di warnet biasanya terpasang program pelindung semacam Deepfreeze, Returnil, Shadow Defender, Clean Slate, dan sejenisnya. Kalau pun ada virus yang aktif, sepanjang admin warnet "tidak membuat kekacauan" dengan memasukkan virus/worm di dalam proteksi Deepfreeze, maka begitu komputer di-restart, virus yang ada di drive aktif (biasanya di drive **C**) akan ditendang keluar. Lain halnya jika admin yang sengaja/ tanpa sengaja justru mengamankan virus di dalam Deepfreeze, tentu lebih rumit lagi urusannya.

Jadi, yang umumnya terjadi: setelah komputer di-restart, virus mungkin masih ada di drive data, drive D, E dan sebagainya, tetapi filenya tidak aktif, karena pemicunya di C sudah tidak ada. Proses yang berjalan juga sudah tidak ada –sehingga file virus bisa dihapus. Upaya virus meng-

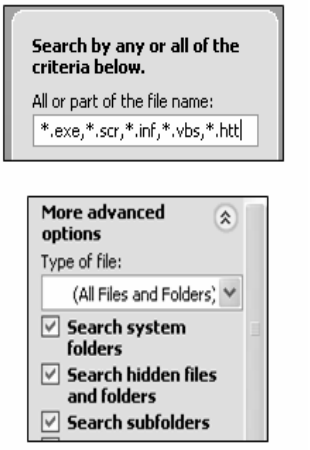
hidupkan diri bersamaan dengan masuk Start Up Windows juga gagal, karena sudah ditendang duluan oleh Deepfreeze atau program sejenis.

Jadi, dalam kasus di warnet, jurus jari sakti, penulis rasa lebih aman ketimbang repot membunuh satu demi satu pemicu virus memakai Process Explorer, Security Task Manager, Unlocker, atau program kill yang lain.

Setelah pemicu virus terbunuh dengan sukses karena ditendang oleh Deepfreeze atau Returnil, langkah berikutnya mudah saja, kita cari file-file yang secara kasat mata kita duga itu adalah worm atau virus, lalu kita hapus.

Cara gampangnya ya kita pakai **Find** atau **Search**. Jika fitur Find/Search di blokir entah oleh admin warnet atau bisa juga oleh worm itu sendiri, kita buka dulu proteksinya atau bisa juga kita pakai program Find/Search dari luar yang bisa dicari di internet.

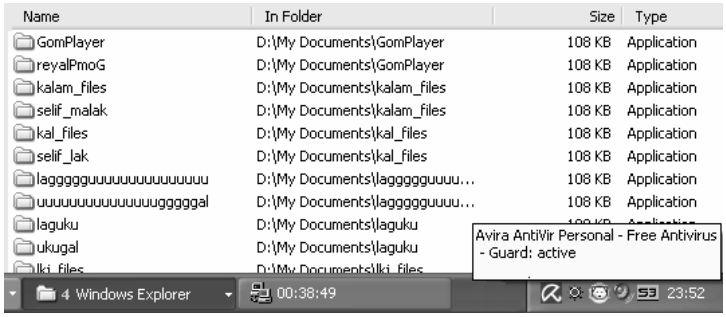
Anggap saja kita telah dengan sukses memanggil Find/Search milik Windows.



Gambar 2.31 Cari file exe, scr, vbs dan sebagainya

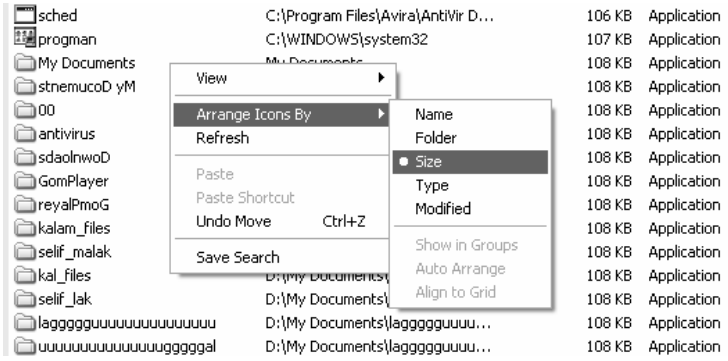
1. Kita isikan jenis file yang ingin kita cari, terutama file .exe. Tambahkan juga file-file lain yang sering kali berbahaya, seperti .vbs, .inf, dan sebagainya. Pilih target lokasi yang ingin dicari. Pilih juga dengan Advanced Options-nya: **Search Hidden Files**.

2. Karena kebetulan di komputer yang penulis pakai, yang ada adalah file .exe yang mirip dengan tampilan worm atau virus-virus lokal, maka yang tampak di hasil **Search** juga file-file tersebut.



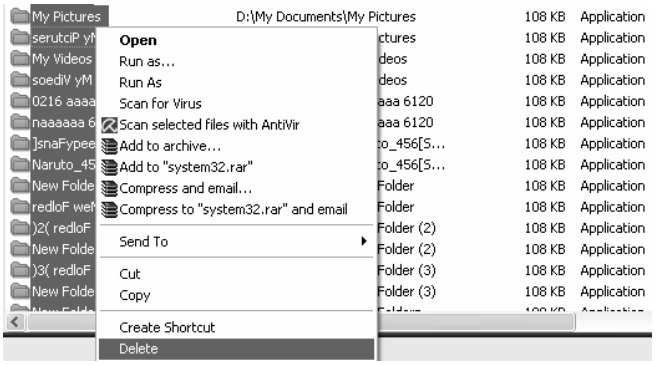
Gambar 2.32 Hasil pencarian

3. Urutkan file-file tersebut sesuai ukuran, agar mudah dihapus. Klik kanan **Arrange Icons by Size**.



Gambar 2.33 Urutkan berdasarkan ukuran

4. Blok file-file yang kita curigai sebagai worm. Gunakan **Shift+ tombol panah** pada keyboard, atau **Shift+Page Down** untuk memblok, lalu **Delete**.



Gambar 2.34 Hapus file

Dalam kasus di warnet, kita tidak perlu terlalu repot menutup file virus tersebut dengan program Kill Process semacam Security Task Manager, Process Explorer, Hijack This, dan sejenisnya. Kita juga tidak perlu terlalu pusing memikirkan di mana pemicu virus tersebut, apakah di registry atau di tempat lain. Ini karena ketika komputer di-restart, semuanya kembali ke kondisi semula. Yang kita pikirkan sederhana saja, bagaimana caranya agar komputer yang kita pakai pada sesi itu menjadi sedikit lebih aman dan nyaman. Kalaupun ada worm di situ, jangan sampai worm itu kita jadikan oleh-oleh, malah kita bawa pulang ke rumah sehingga membuat komputer di rumah menjadi "tercemar" virus. Bukan salah Anda jika Anda membersihkan terlebih dahulu virus/malware di komputer yang Anda pakai.

Dalam kasus di warnet, tebak-tebakan keberadaan malware, misalnya saja regedit di-disable, Folder Options hilang, Run hilang, Search hilang, dan sebagainya tidak bisa dijamin kepastiannya. Karena bisa saja yang melakukan blokir memang virus atau worm, tetapi tidak menutup

kemungkinan proteksi itu tidak dilakukan oleh virus tetapi justru dilakukan oleh admin warnet. Bahkan dalam kasus blokir ke situs security tertentu (misalnya Conficker pernah memblokir situs antivirus termasuk virustotal.com dan situs Microsoft) tetap masih ada kemungkinan pelakunya bisa admin/pengelola warnet atau bisa virus, karena beberapa program remote jaringan/remote desktop ada juga dianggap bermasalah oleh antivirus tertentu sehingga situs tertentu bisa saja malah diblokir oleh admin.

Beberapa pengelola warnet mungkin berpikir, ada baiknya jika mereka tahu apa yang dilakukan pengguna sehingga mereka menginstal program pemantau. Sebagian program semacam ini dideteksi berbahaya oleh antivirus atau situs security tertentu, sehingga masih sangat mungkin justru admin memblokir situs/program tertentu.

Karena itulah analisis manual kehadiran virus di komputer warnet menjadi lebih tidak pasti. Karena pada dasarnya kita tidak tahu apakah kondisi komputer yang ada di depan kita memang sengaja dikondisikan demikian oleh pengelolanya atau oleh admin, atau memang pelakunya justru virus atau worm. Jadikanlah mata Anda sebagai alat bantu Antivirus/Anti Malware, tetapi tentu bukan satu-satunya cara mengenali virus. Jadi, ada kombinasi antara pengamatan manual dan antivirus.

2.6 Mencegah Penularan Virus via USB Flash Disk

Penularan virus/malware melalui Flash Disk semakin meningkat akhir-akhir ini. Bagi Anda rekan-rekan yang sering memakai komputer umum termasuk warnet, ada baiknya mewaspadai kemungkinan penularan virus dari warnet atau komputer umum lain ke komputer pribadi di rumah.

Ada dua prinsip dalam mencegah penularan virus melalui USB Flash Disk.

- Pertama: Mencegah virus yang mungkin ada dalam sebuah komputer "mencemari" USB Flash Disk. Dalam kasus di warnet, ini berarti menjaga agar USB Flash Disk milik kita tidak tercemari oleh virus/malware yang mungkin ada di warnet.
- Kedua: Bagaimana mencegah agar komputer yang kita pakai, tidak tertular virus dari USB Flash Disk. Mungkin dalam sebuah USB Flash Disk terdapat virus/malware yang autorun. Kita harus mencegah agar virus tersebut tidak menular ke dalam komputer pribadi kita.

Kedua cara tersebut tentu lebih baik jika dikombinasikan. Ada kemungkinan meskipun USB Flash Disk kita aman, tetapi karena komputer/laptop kadang kala dipakai teman/adik/pacar maka tanpa sengaja mereka menularkan virus dari USB Flash Disk mereka ke komputer kita. Jadi, lebih afdol jika kedua prinsip pencegahan tersebut dikombinasikan.

Jika Anda kebetulan menemukan Flash Disk yang tertinggal di warnet, lebih baik serahkan kepada Operator untuk dikembalikan kepada pemiliknya, ketimbang Anda bawa ke rumah. Bisa saja Anda bermaksud baik mencoba mengidentifikasi pemilik Flash Disk dan mengembalikannya secara personal, misalnya ingin *ngajak kenalan* ☺, tetapi itu meningkatkan risiko komputer Anda tercemar virus.

Proteksi dengan cara pertama (mencegah virus masuk ke Flash Disk) bisa dilakukan dengan berbagai cara, misalnya dengan mencegah malware membuat file aktivasi virus (file autorun.inf) di USB Flash Disk, mencegah penulisan/akses ke USB Flash Disk (membuat Flash Disk jadi read only), memasang penghalang ber-password untuk mengakses isi Flash Disk sehingga virus atau bahkan orang lain tidak bisa mengambil/menulis

data. Jika perlu melakukan scan dengan antivirus portable yang diletakkan di luar folder/kontainer terproteksi.

NB: Beberapa model Flash Disk yang biasanya berharga lebih mahal dari model lainnya, memiliki semacam tombol (*write proctection switch*), yang bisa membuat Flash Disk dalam kondisi *read only*. Ada juga Flash Disk yang sudah terintegrasi dengan program security bawaan, sehingga akses ke Flash Disk bisa dibatasi dengan memasang password. Memang bagus memiliki Flash Disk semacam itu. Tetapi bila kebetulan kita memakai Flash Disk biasa saja, kita tetap bisa juga melakukan tambahan proteksi dengan aneka tool yang bisa kita download di internet.

Proteksi dengan Cara Kedua (mencegah virus di Flash Disk menular ke komputer) bisa dilakukan dengan berbagai cara, misalnya mencegah file autorun bisa berjalan di komputer terkait. Ini bisa dilakukan dengan manipulasi registry atau dengan bantuan software. Bisa juga dilakukan dengan mengunci port USB, scan otomatis terhadap USB Flash Disk, atau analisis file autorun yang mungkin ada dalam USB Flash Disk. Penguncian terhadap port USB bisa dilakukan berbasis perangkat, misalnya memasang sejenis gembok di port USB atau yang lebih umum adalah memakai software security atau manipulasi registry.

Ada banyak program serta banyak trik yang bisa dipakai untuk proteksi cara pertama, proteksi cara kedua, maupun kombinasi keduanya.

Berikut ini aneka proteksi memakai cara pertama:

- Proteksi Autorun.inf dari Antivirus Smadav.
- Proteksi manual dengan membuat folder Autorun.inf, dengan membuat folder memakai karakter ilegal atau karakter ASCII tertentu, atau trik manual lain.

- Memakai software Panda USB Vaccine, BitDefender USB Immunizer, USB Write Protect, USB Write Protector, Pen Protector, Thumb Screw, atau Flash Disk Desinfector.
- Memakai Flash Disk Lock atau USB Safe Guard untuk mem-password Flash Disk.
- Dan masih banyak lagi.

Aneka proteksi cara kedua bisa dilakukan, antara lain dengan:

- Melakukan manipulasi registry secara manual, bisa lewat regedit atau gpedit.msc atau script tertentu untuk mencegah file autorun berjalan.
- Memakai program USB Defender, USB Port Locked, Ninja Pen Drive, Autorun Virus Remover, USB Disk Security, USB Threat Defender, AutoRun Protector, atau USB Firewall.
- Memakai aneka antivirus yang dibuat khusus untuk men-scan USB Flash Disk dikombinasikan dengan Antivirus biasa.
- Memakai program security yang memblokir eksekusi file, seperti Anti Executable.
- Memakai program sejenis Deepfreeze, Returnil, dan program Sand Box lainnya.

Semua cara di atas oke-oke saja, dan bagusnya lagi program proteksi USB banyak yang gratis –full freeware, sehingga kalau mau Anda bisa mencoba masing-masing program.

Untuk mencegah virus menciptakan file autorun.inf di Flash Disk, penulis memakai program USB Defender. Program ini akan membuat ikon folder dengan nama autorun.inf, yang sulit dihapus dan digantikan file virus. USB Defender bisa Anda download di alamat:

http://sites.google.com/site/mbentefor/ atau di alamat: http://www.softpedia.com/get/Antivirus/USB-Defender.shtml.

Gambar 2.35 Download USB Defender

Cara memakai program ini super mudah. Kita ekstrak file hasil download, lalu kita jalankan file executable. Cuma ada dua tombol, yaitu **Protect** dan **Unprotect** sehingga rasanya siapa pun dapat memakai program ini dengan baik dan benar. Pastikan Flash Disk sudah Anda colokkan ke port USB. Jalankan program USB Defender lalu kita klik tombol **Protect**.

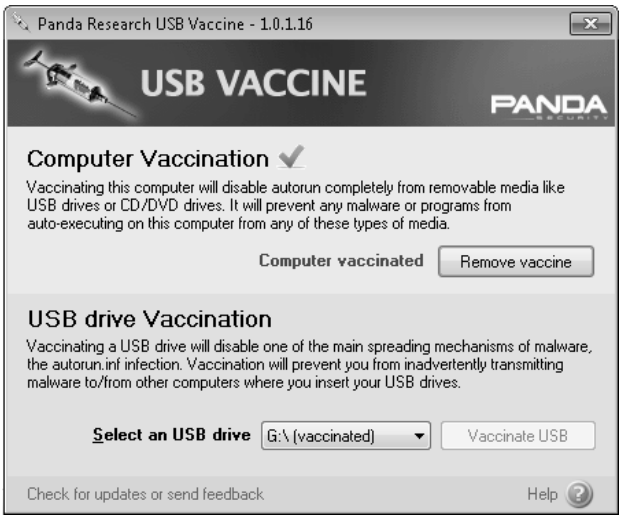
Gambar 2.36 Centang Pro method, klik tombol Protect

Pastikan checkbox bertuliskan **Pro method (you must be administrator!)** telah Anda centang untuk proteksi yang lebih maksimal. USB Defender akan membuat folder **Autorun.inf** dengan proteksi 5 level yang sulit dihapus oleh virus.

Gambar 2.37 Proteksi autorun.inf di FlashDisk telah dibuat

Gambar 2.38 Tampilan Autorun.inf karya USB Defender yang sulit dihapus

Selain memakai USB Defender, Panda USB Vaccine juga merupakan alternatif proteksi USB FlashDisk yang cukup baik. Program ini bisa di-download di: http://www.softpedia.com/get/Security/Security-Related/Panda-USB-Vaccine.shtml.



Gambar 2.39 Panda USB Vaccine

Cara memakainya, instal dulu program ini. Untuk melindungi komputer, pada bagian **Computer Vaccination**, klik tombol **Vaccinate Computer** untuk memproteksi komputer dari kemungkinan berjalannya file autorun.inf dari Flash Disk.

Sedangkan untuk melindungi USB Flash Disk dari pembuatan file autorun.inf virus, klik tombol **Vaccinate USB**. Program ini memiliki kelebihan karena mempunyai dua kemampuan sekaligus, yaitu melindungi komputer dari virus yang ada di Flash Disk serta melindungi Flash Disk dari virus yang ada di komputer.

Dengan mencegah berjalannya file autorun.inf, tentu bukan berarti USB Flash Disk aman 100 persen. Hal ini karena walaupun file autorun.inf diproteksi, bila kebetulan komputer warnet bervirus aktif, tetap ada kemungkinan file-file worm atau virus di-copy-kan ke Flash Disk. File tersebut memang tidak otomatis berjalan atau non-aktif, tetapi jika secara tidak sengaja tersenggol, atau dibuka, maka virus akan aktif. Karena itu, proteksi semacam ini tetap harus dikombinasikan dengan antivirus.

Proteksi yang dibuat program security, sebenarnya mungkin saja dibuat sendiri secara manual. Misalnya proteksi "Vaccinate Computer" dari Panda, sebenarnya dilakukan dengan manipulasi registry yang tidak terlalu sulit. Jika dilihat file reg-nya, kurang lebih seperti ini:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

Buat saja tulisan di atas dengan Notepad, lalu simpan dengan ekstensi .reg, lalu jalankan file .reg tersebut.

Program lain seperti Bit Defender USB Immunizer memproteksi autorun dengan alamat registry lain lagi:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\Explorer]
"NoDriveTypeAutoRun"=dword:00000004
```

Walaupun memang sangat mungkin melakukan proteksi autorun secara manual, tetapi memakai program security tentu memiliki kelebihan dari sisi kemudahan pemakaian. Beberapa program seperti Panda USB Vaccine juga berjalan di belakang layar, sehingga bisa mendeteksi ketika sebuah USB Flash Disk dicolokkan di port USB.

2.7 Tip Menghindari Virus/Worm di Warnet

Berikut ini sejumlah tip sederhana untuk menghindari virus atau worm dari warnet:

- Jika memungkinkan, pilihlah warnet yang punya reputasi baik. Warnet dengan bangunan yang baik, ruangan bersih, nyaman, biasanya juga baik pula pemeliharaan komputer mereka. Mereka memerhatikan pelanggannya dalam berbagai aspek.
- Jika Anda tidak bermaksud menyimpan data di komputer warnet, sebaiknya pilihlah warnet yang menghapus data pengguna secara periodik. Saran penulis, jangan memilih warnet yang langsung menghapus data begitu komputer restart, karena selalu ada kemungkinan Anda malah kehilangan data yang Anda simpan di harddisk. Tetapi pilihlah warnet yang menghapus data ketika pengguna selesai menggunakan komputer di warnet tersebut.
- Pilih juga warnet yang otomatis me-restart komputer pengguna yang sudah selesai memakai internet (ketika pengguna log out dari Billing, maka komputer kemudian di-restart). Selain lebih aman dari para virus, privasi dan data Anda sedikit lebih

terjamin, karena kalau pun Anda lupa log out dari suatu situs internet, maka Deepfreeze atau program sejenisnya akan membantu membuang jejak-jejak Anda.

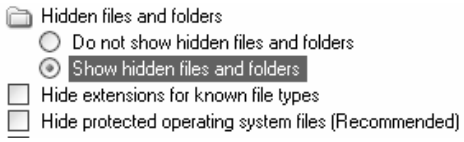
- Jika warnet yang Anda kunjungi tidak melakukan itu, lakukan restart secara manual sebelum dan setelah memakai internet. Restart sebelum memakai internet bertujuan untuk mem-bersihkan program antik yang mungkin diinstal oleh pengguna sebelum Anda. Sedangkan restart setelah memakai internet bertujuan untuk menghapus semua jejak Anda, cookie, dan lain-lain. Dengan asumsi di warnet tersebut terpasang DeepFreeze atau teman-teman sejenisnya. Harapan penulis sih semoga warnet-warnet langsung melakukan itu.

- Pilihlah warnet yang ada antivirusnya, yang ideal setidaknya ada kombinasi dari antivirus internasional dan antivirus lokal. Kebanyakan antivirus lokal cukup baik untuk menghadapi worm atau virus-virus lokal. Dan warnet boleh dikatakan salah satu ajang unjuk gigi produsen virus lokal. Pastikan antivirus di warnet tersebut sudah ter-update atau Anda lakukan update sendiri jika perlu. Jika memang terpaksa di komputer tidak terpasang antivirus, pakailah antivirus portabel. Selalu simpan setidaknya satu antivirus portabel di Flash Disk Anda. Karena sifat portabelnya, Anda mau menyimpan beberapa antivirus juga tidak jadi masalah.

- Jika di warnet tersebut memungkinkan untuk menyimpan data, jangan terlalu usil dengan browsing folder-folder milik orang lain. Ingat bahwa virus atau worm bisa menyamar jadi apa saja, termasuk menyamar jadi ikon folder, file word, file jpg, dan sejenisnya. Perhatikan type data dan ukurannya. Folder beneran tidak punya ukuran. Pada type data tulisannya adalah file folder.

Jika ada folder yang ada ukurannya atau type datanya tulisannya adalah application, maka bisa dipastikan itu bukan folder beneran, tetapi file worm yang menyamar jadi folder. Perhatikan juga bila ada file yang ukuran-ukurannya sama. Pilih **View detail** untuk membantu melihat kondisi ini.

Gambar 2.40 Memerhatikan file dan folder

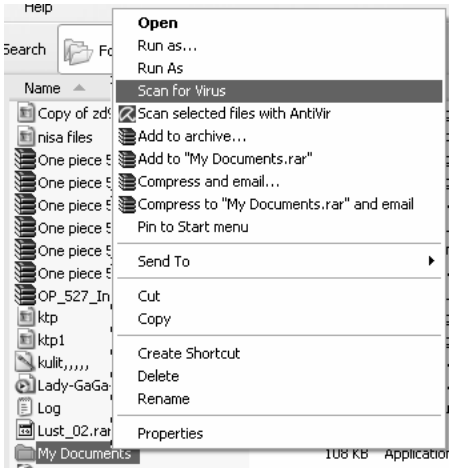


Gambar 2.41 Show hidden di folder Options

- Worm atau virus lokal biasanya senang memakai ekstensi ganda untuk menyamarkan dirinya. Jika memungkinkan, tampilkan ekstensi di komputer tersebut melalui **Folder Options**-nya. Biarkan kosong pada **Hide extensions for known file types**. Selain itu, tampilkan juga **Hidden file** dan **Operating system file** untuk mempermudah membedakan.

- Berhati-hatilah jika ingin men-scan sebuah file memakai menu klik kanan software antivirus, karena ada virus yang memakai juga cara itu sebagai semacam backup aktivasi andai virus itu dinonaktifkan atau anak-cucunya dihapus. Ekstensi file yang secara normal tidak berbahaya bisa saja di-*redirect* atau dibelokkan sesuai kepentingan. Jadi, selain mamakai ekstensi ganda, bisa saja pembuat virus membuat juga satu file yang

ekstensinya secara normal tidak berbahaya, tetapi sudah dibelokkan registry-nya. Untuk melengkapi penderitaan itu, bisa juga dibuatkan semacam menu context atau klik kanan untuk menipu pengguna. Perhatikan teknik salah satu worm yang penulis temukan di sebuah warnet: Tulisan **Scan for virus** pada menu klik kanan tidak berasal dari antivirus, tetapi sebaliknya menu itu sendiri justru dibuat oleh Sang Virus. Pada Gambar 2.42, menu klik kanan yang beneran dibuat oleh software antivirus adalah menu yang di bawahnya, yang dibuat oleh antivirus Avira.



Gambar 2.42 Hati-hati dengan menu klik kanan

- Agar lebih aman, restart komputer untuk memastikan tidak ada program aneh yang dipasang oleh manusia yang tidak berhak. Tetapi harap diingat bahwa DeepFreeze hanya menendang program yang diinstal di luar proteksi DeepFreeze. Biar pun kebanyakan admin itu baik hati ☺, masih ada kemungkinan admin memasang program aneh-aneh, baik untuk kemudahan pengaturan, admin tidak percaya 100 persen pada pengguna

sehingga ingin mengamati aktivitas pengguna, atau “alasan lain” entah positif atau negatif. Begitu juga ingatlah selalu masih sangat mungkin DeepFreeze di-hack oleh pengunjung warnet dan mereka menginstal atau meletakkan program aneh-aneh di warnet (misal virus atau keylogger).

- Setelah komputer di-restart, hapus saja file-file mencurigakan di folder data. Gunakan Find/Search bila perlu. Buka proteksi Find jika diproteksi, atau gunakan program pencari eksternal. Ada banyak program pencari di internet. Cari ekstensi-ekstensi yang berbahaya semacam .exe, v.bs, .bat, .inf, dan sebagainya. Hapus file-file yang Anda anggap berbahaya. Bukan kewajiban Anda mempertahankan data orang lain, apalagi bila jelas-jelas ke-mungkinan beberapa file adalah worm atau malware. Jika virus di folder data tidak Anda hapus, ada kemungkinan Anda main senggol-senggolan dengan virus tersebut.
- Jangan membuka situs yang aneh-aneh. Jika Anda *maksa* pengen membuka situs-situs ajaib semacam situs porno, warez, penyedia serial number, bajakan, dan sebagainya –pastikan Anda tahu konsekuensinya. Saran penulis, jika Anda memang sangat membutuhkan keberadaan situs-situs antik tersebut, buatlah jeda berinternet yang baik. Misalnya saja jam-jam awal Anda pakai untuk hal yang normal, membuka email, chatting, blogging, download, dan sebagainya. Scan file hasil download dengan antivirus entah itu antivirus yang terinstal atau portabel. Jika perlu upload file penting hasil download ke multiple antivirus online semacam virustotal.com. Selanjutnya Anda restart saja komputer entah dengan cara apa –baru Anda simpan data yang Anda download ke Flash Disk. Jika di warnet ada DeepFreeze, ini akan lumayan mengurangi efek, baik virus

lokal maupun virus internasional yang menyusup atau aktif, baik secara langsung maupun lewat situs-situs tertentu. Sebagai catatan, pastikan dahulu bahwa di warnet itu data tidak otomatis hilang ketika komputer di-restart.

- Untuk mencegah aktivasi virus di USB Flash Disk, Anda bisa memperaman USB Flash Disk dengan fitur Smad Lock dari antivirus Smadav (http://www.smadav.net/), memakai program USB Defender (http://www.softpedia.com/get/Antivirus/USB-Defender.shtml), Panda USB Vaccine (http://www.pandasecurity.com/homeusers/downloads/usbvaccine/), atau USB Immunizer (http://labs.bitdefender.com/?page_id=108). Tool-tool tersebut mencegah penularan virus/malware memakai file autorun.inf.
- Lebih bagus lagi jika di rumah Anda, di komputer pribadi, Anda instal juga program pemblokir USB, serta Deepfreeze, atau sejenisnya. Deepfreeze meskipun program yang "sangat warnet", juga berguna dipasang di komputer pribadi. Tentu Anda bisa mencoba memakai program sejenis seperti Wondershare Time Freeze, Shadow Defender, Rollback RX, Returnil, ToolWiz Time Freeze, dan lain sebagainya.