Memburu Virus Rontokbro Dan Variannya Dalam Membasmi Dan Mencegah

Junaidi
junaidiskom@yahoo.com
http://junaidiskom.wordpress.com

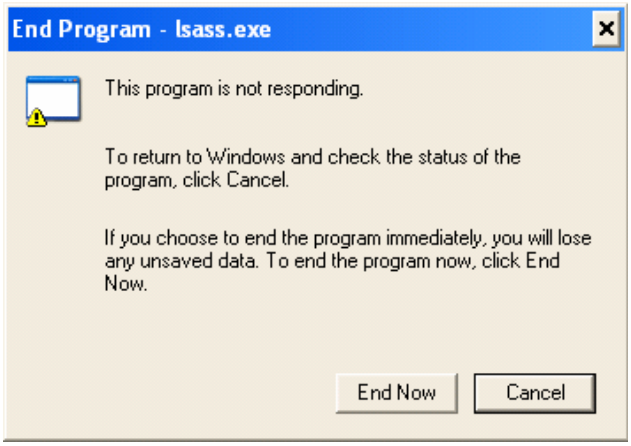
Abstraksi

Cepatnya perkembangbiakan virus rontokbro (kerap kali disebut-sebut dengan virus brontok) membuat seluruh pengguna computer merasa kesal, apabila komputernya berjalan sangat lambat tidak seperti biasanya. Hal ini secara sadar maupun tidak sadar mungkin saja telah terinfeksi virus, satu diantaranya adalah rontokbro yang beberapa bulan terakhir sedang gencar-gencarnya menyerang computer kita. Virus rontokbro atau yang diberi nama W32/Rontokbro@mm selalu membuat aktifitas kerja hardisk tanpa henti, hal ini dapat dilihat pada lampu indicator hardisk terus berkedip, menandakan bahwa hardisk sedang bekerja karena virus rontokbro sedang menjalankan aktifitasnya dalam memperbanyak diri. Dilihat dari namanya, dan pesan moral yang disampaikan oleh virus ini, rontokbro adalah virus local buatan hacker Indonesia, yang penyebaranya telah mendunia dan tegolong virus kelas 2 dan memiliki SMTP (Simple Mail Transfer Protocol) sendiri. Virus ini mampu menyebarkan dirinya dengan email masal (mass mailing) dan menghapus anggapan virus lokal yang mengandalkan media penyimpanan yang berpindah-pindah dari satu computer ke computer lainnya sebagai sarana penyebaran. Virus ini menyebar ke pengguna computer di Indonesia atau Asia Tenggara yang terkoneksi dengan internet. Pada saat ini, para pengguna internet Indonesia dan di belahan dunia lain seperti Jepang, Spanyol, Polandia, Amerika, Vietnam, Belanda, Swedia, Hungaria, Rusia, Peru dan Israel juga kebagian aksi virus rontokbro. Adapun kelebihan virus rontokbro adalah kemampuannya dalam rekayasa sosial yang cukup tinggi. Teknik penyerangan virus ini dengan memalsukan icon (menggunakan icon folder) dirinya sebagai file tidak berdosa, melakukan bloking akses terhadap registry editor, microsoft configuration, command prompt, setting folder option, situs security tertentu, melakukan restart computer secara otomatis. Guna menghindari deteksi cepat oleh vendor sekurity, virus ini selektif dalam mengirimkan email dirinya.

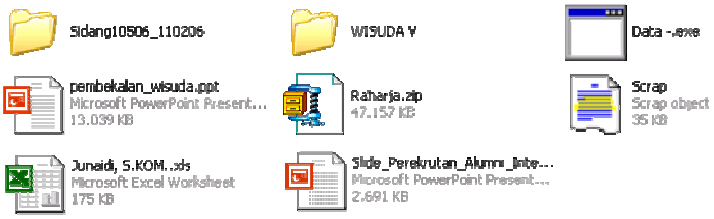
Kata Kunci : Virus, *Registry*, Brontok, Rontokbro

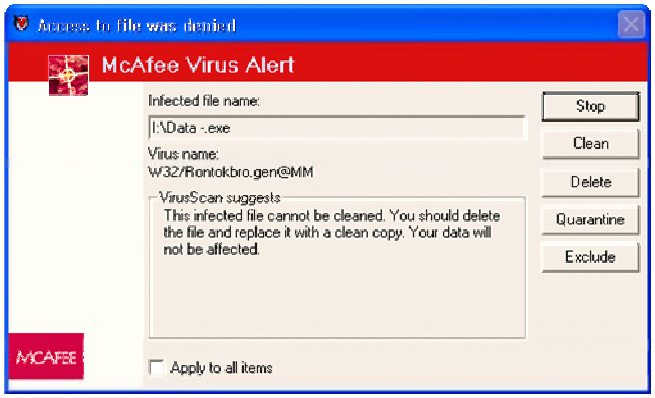
Pendahuluan

Berawal dari *computer* penulis, dimana lampu *indicator hardisk* terus berkedip, yang menandakan *hardisk* terus bekerja, menyebabkan proses menjadi sangat aneh dan lambat dari biasanya. Seperti biasanya penulis selalu melakukan *logoff* atau *restart* untuk menormalkan kembali penggunaan memori, dengan asumsi akan berjalan dengan baik dan lebih cepat, namun anehnya setelah menekan tombol *logoff* atau *restart*, *computer* tidak melakukan aktifitas seperti biasanya, ia selalu menampilkan pesan permintaan untuk menghentikan program secara paksa, menandakan bahwa ada aktifitas program yang sedang berjalan, padahal tidak ada satupun program yang sedang berjalan. Hal ini selalu dilakukan berulang–ulang dengan aktifitas proses yang berbeda-beda, walaupun telah dilakukan penghentian secara paksa dengan menekan tombol *end now*. Ini menandakan ada beberapa proses yang berjalan dengan diam-diam tanpa kita sadari, misalnya saja permintaan penghentian proses *smss.exe*, *csrss.exe*, *isass.exe*, *winlogon.exe*, *services.exe*. Hal ini menyebabkan *computer* tidak mau melakukan *logoff* atau *restart* apalagi *shutdown*, keculai dilakukan secara paksa dengan menekan tombol *reset* atau *power*, bahkan lebih ekstrim lagi jika tetap tidak mau melakukan *shutdown* atau *restart*, lakukan pemutusan terhadap arus listrik, misalnya saja mencabut kabel *power*, mematikan *stabilizer* dan lain sebagainya, tergantung tingkat kekesalan *user*.



Gambar 1 : *Komputer tidak mampu melakukan logoff atau restart karena ada rontokbro sedang aktif*





Gambar 2 *: File buatan tontokbro yang tertangkap oleh Antivirus McAfee*

Seperti biasanya, kalau computer penulis terkena virus, penulis selalu melakukan pelacakan / pemburuan untuk mengetahui teknik penyebarannya, sebelum dilakukan *scaning* dengan antivirus, harapan penulis adalah dapat menangkap file inti dari penyebaran virus rontokbro, dan dapat membuka *source code* seperti yang sebelum-sebelumnya pernah dilakukan, Dan biasanya kalau berhasil mengetahui teknik penyebarannya, bahkan mendapatkan file inti serta *source code* nya penulis tidak membutuhkan lagi antivirus untuk membasminya, karena dapat dilakukan secara manual dengan menggunakan *bootable* terpisah serta menghapus file-file inti dari virus tersebut, tentunya hal ini dapat dilakukan kalau kita berhasil melacak keberadaan file tersebut sesuai ciri-ciri dan teknik

penyerangan virus tersebut. Jika berkesempatan terkadang penulis membuat antivirus sendiri dengan menggunakan program aplikasi yang dikuasai, tentunya dengan pola-pola sederhana, yaitu *searching, question, actions* dimana *actions* itu sendiri mengandung langkah *moving* atau *deleting*, belum sampai pada tahap maintenance file.

Hasil Dan Pembahasan

Media Penyebaran Virus Rontokbro

Seperti yang pernah dijelaskan sebelumnya, bahwa virus rontrokbro memiliki beberapa kehebatan, selain media penyebaran sangat cepat melalui email masal lewat internet, juga memiliki *simple mail transfer protocol (SMTP)* sendiri, dan yang menjadi sasaran adalah Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP. Berikut adalah contoh dari detail email yang mengandung virus rontokbro yang penulis dapatkan :

From: [Dipalsukan]
Subject: kosong
Message:
BRONTOK.A [By: HVM**-Jowo*** #** Community]
-- Hentikan kebobrokan di negeri ini --
1. Adili Koruptor, Penyelundup, Tukang Suap, Penjudi, & Bandar NARKOBA
(Send to "NUSAKAMBANGAN")
2. Stop Free Sex, Absorsi, & Prostitusi
3. Stop (pencemaran laut & sungai), pembakaran hutan & perburuan liar.
4. SAY NO TO DRUGS !!!
-- KIAMAT SUDAH DEKAT --
Terinspirasi oleh: Elang Brontok (Spizaetus Cirrhatus) yang hampir punah[By: HVM**-Jowo*** #** Community--
Attachment:
Kangen.exe

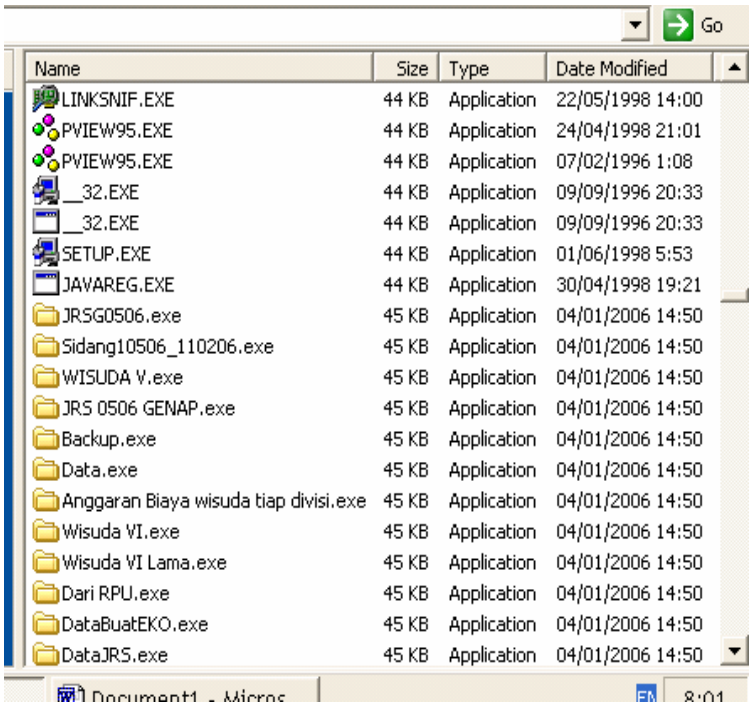
***Gambar 3** : Detail email yang mengandung rontokbro berupa pesan moral dan attachmen virus kangen*

Jika kita perhatikan email diatas, jelas pembuat virus tersebut memiliki kepakaan sosial yang tinggi, dimana ia menyampaikan pesan-pesan moral yang saat ini sedang hangat-hangatnya dibicarakan di Indonesia. Dan kalau penulis boleh berspekulasi berdasarkan email tersebut, hacker rontokbro berasal dari pulau jawa, berdasarkan pada awal tulisan dan akhir tulisan yang ditutup dengan Jowo–Community.

Kalau kita perhatikan *attachment* email tersebut, rontokbro melampirkan file kangen.exe, dimana ini telah sama-sama kita ketahui merupakan virus yang sebelumnya juga sempat menguasai hampir sebagian pengguna computer didunia yang juga berasal dari Indonesia, virus kangen.exe ini dalam pernyebarannya menggunakan icon microsoft word dengan (extension .exe), dimana namanya akan selalu berubah-ubah sesuai file word yang kita buka atau buat.

Virus Rontokbro vs Virus Kangen

Melihat dari *attachmen* yang dilampirkan oleh *email* bervirus rontokbro, lantas muncul pertanyaan dari ini?, apakah pembuat virus rontokbro juga pembuat virus kangen!, saya juga tidak dapat memastikan, yang pasti virus rontokbro menggambarkan pesan-pesan moral yang cukup tinggi, sementara virus kangen menyampaikan kerinduan seseorang sedang jatuh cinta, pada syairnya tersirat dalam lirik lagu kangen. Namun demikian ada kemiripin diantara keduanya, misalnya saja melihat dari teknik penyebarannya, dan cara-cara proses manipulasinya untuk perkembangbiakan virus tersebut. Seperti halnya virus rontokbro melakukan manipulasi icon dan extension exe dan virus kangen pun demikian, bedanya adalah kalau virus rontrokbro menggunakan icon folder sementara kangen menggunakan icon microsoft word. Dalam penamaan virus rontrokbro menggunakan nama file dari yang pernah dibuka, demikian juga dengan virus kangen. Virus rontokbro dan virus kangen sama-sama memblokir fasilitas registry editor, Microsoft configuration, folder option. Virus rontokbro dan virus kangen sama-sama menggunakan hidden file. Virus rontokbro dan kangan sama-sama menggunakan nama awalan W32/, dan masih banyak lagi perbedaan dan persamaanya, namun jika dilihat dari teknik penyebarannya keduanya mempunyai kemiripan. Bisa jadi pembuat virus rontokbro sama dengan pembuat virus kangen, atau pembuat virus rontokbro hanyal ingin mendompleng ketenaran dari nama virus kangen yang telah mendunia.

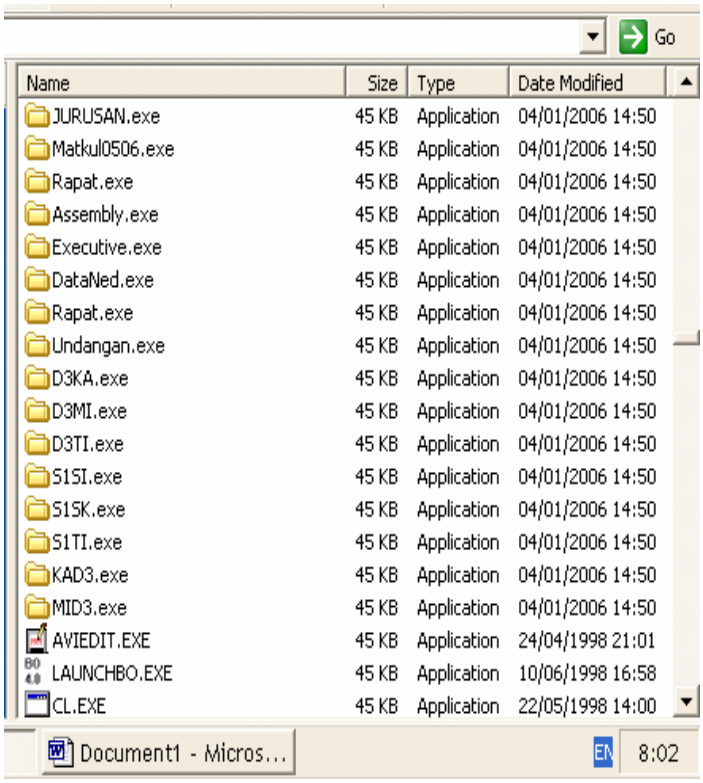


***Gambar 4** : File dengan icon folder dan type appication berukuran 45 KB, dengan date modified 04/01/2006 14:50 menandakan bahwa ini adalah file ciptaan dari rontokbro.*

Virus Rontokbro Adalah Virus Pintar Dan Konsisten

Kepintaran dari virus rontokbro, ia mampu menghindari setiap aksi yang ditujukan untuk pemusnahan dirinya, misalanya saja dengan kemampun virus rontokbro untuk melakukan *restart* jika saja dia merasa aktivitsnya sedang diusik atau akan dibasmi oleh antivirus lain. Kemampuan virus rontokbro untuk melakukan *restart* secara otomatis dapat penulis ketahui ketika penulis mencoba melakukan pemburuan dan pembasmian secara manual, dengan mencoba memasuki bagian-bagian vital tertentu pada system registry, microsoft configuration, command prompt, folder option pada windows explorer, autoexec.bat dan masih banyak lagi. Bahkan virus rontrokbro akan melakukan restart secara otomatis ketika ada aktivitas CD maupun file yang dicurigai akan mengancamnya. Kemampuan virus rontrokbro dalam melakukan restart bukan lah semata-mata karena kemampuan intelegennya, melainkan ia telah

mendaftarkan berbagai nama, yang menjadi ancaman, sehingga ketika menemukan kesesuai nama file dengan nama file yang telah diinventarisir, secara otomatis akan dilakukan restart. Berikut adalah beberapa nama yang diblokir oleh virus rontokbro : ***..; .@; @.; .ASP; .EXE; .HTM; .JS; .PHP; ADMIN; ADOBE; AHNLAB; ALADDIN; ALERT; ALWIL; ANTIGEN; APACHE; APPLICATION; ARCHIEVE; ASDF; ASSOCIATE; AVAST; AVG; AVIRA; BILLING@; BLACK; BLAH; BLEEP; BUILDER; CANON; CENTER; CILLIN; CISCO; CMD.; CNET; COMMAND; COMMAND PROMPT; CONTOH; CONTROL; CRACK; DARK; DATA; DATABASE; DEMO; DETIK; DEVELOP; DOMAIN; DOWNLOAD; ESAFE; ESAVE; ESCAN; EXAMPLE; FEEDBACK; FIREWALL; FOO@; FUCK; FUJITSU; GATEWAY; GOOGLE; GRISOFT; GROUP; HACK; HAURI; HIDDEN; HP.; IBM.; INFO@; INTEL.; KOMPUTER; LINUX; LOG OFF WINDOWS; LOTUS; MACRO; MALWARE; MASTER; MCAFEE; MICRO; MICROSOFT; MOZILLA; MYSQL; NETSCAPE; NETWORK; NEWS; NOD32; NOKIA; NORMAN; NORTON; NOVELL; NVIDIA; OPERA; OVERTURE; PANDA; PATCH; POSTGRE; PROGRAM; PROLAND; PROMPT; PROTECT; PROXY; RECIPIENT; REGISTRY; RELAY; RESPONSE; ROBOT; SCAN; SCRIPT HOST; SEARCH R; SECURE; SECURITY; SEKUR; SENIOR; SERVER; SERVICE; SHUT DOWN; SIEMENS; SMTP; SOFT; SOME; SOPHOS; SOURCE; SPAM; SPERSKY; SUN.; SUPPORT; SYBARI; SYMANTEC; SYSTEM; CONFIGURATION; TEST; TREND; TRUST; UPDATE; UTILITY; VAKSIN; VIRUS; W3.; WINDOWS SECURITY.VBS; WWW; XEROX; XXX; YOUR; ZDNET; ZEND; ZOMBIE***.



***Gambar 5** : File dengan icon folder dan type appication berukuran 45 KB, dengan date modified 04/01/2006 14:50 menandakan bahwa ini adalah file ciptaan dari rontokbro.*

Rontokbro dalam menjalankan aktivitas penyerangannya mengalami keunikan, misalnya saja ia akan menghindari alamat-alamat dengan domain sebagai berikut : ***PLASA; TELKOM; INDO; .CO.ID; .GO.ID; .MIL.ID; .SCH.ID; .NET.ID; .OR.ID; .AC.ID; .WEB.ID; .WAR.NET.ID; ASTAGA; GAUL; BOLEH; EMAILKU; SATU***. Dilain sisi virus rontokbro berusaha menyerang website ***ISRAEL.GOV.IL; PLAYBOY.COM, KASKUS.COM; 17TAHUN.COM*** dengan cara membanjiri dengan ping. Namun dampak dari aktivitas ini hanya akan terasa kalau komputer yang terinfeksi mencapai jumlah yang sangat banyak, sehingga pada kasus tertentu dapat mengakibatkan website yang diserang menjadi lumpuh /down.

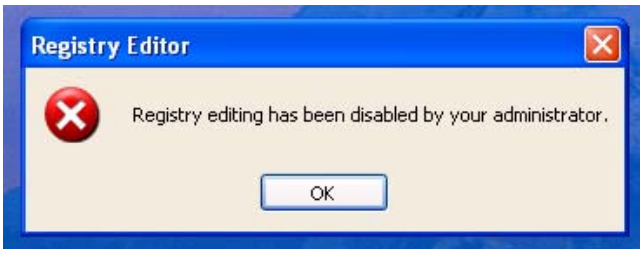
Rontokbro yang disebarkan ke domain di luar Indonesia mencatat "prestasi" yang cukup baik (untuk ukuran Indonesia) dan berhasil menyebar kenegara lain. Hebatnya lagi, antivirus top tidak mengenali virus ini. Versi rontokbro yang dikenali oleh antivirus hanya versi awal W32/Rontokbro.A@mm dan W32/RontokbroB.@mm saja. Padahal varian Rontokbro yang ada dapat dikenali oleh Norman Virus Control sudah sampai varian ke 7 W32/Rontrokbro.G@mm. Satu kehebatan lain dari Rontokbro adalah kemampuannya untuk mencari SMTP server guna mengirimkan kopi dirinya dan ia juga menggunakan SMTP engine sendiri untuk mengirimkan dirinya pada semua alamat email yang berhasil dikumpulkannya dari komputer yang terinfeksi.

Perlindungan Diri Virus Rontokbro Dan Aktivitas Penyerangannya

Untuk menghindari pembasmian, virus rontokbro telah melakukan perlindungan diri dengan sangat baik, adapun perlindungan diri yang dilakukan adalah :

1. Pemblokiran Terhadap Regedit (Registry Editor)

Layaknya seperti virus lainnya, virus rontrobro telah membelokir fasilitas regedit, baik yang dijalankan melalui menu run maupun pengaksesan langsung terhadap aplikasi editing registry. Hal ini dilakukan, kerana memang otak dari pengembangbiakan virus ini berada pada registry untuk memanggil file-file yang ada didalam jaringan virus rontokbro. Ini dapat dibuktikan dengan mengetik regedit pada menu run, atau menjalankan langsung dari explorer, maka secara otomatis computer akan restart.



***Gambar 6** : Fasilitas regeistry editor (regedit) diblokir sebagai salah satu bentuk perlindungan.*

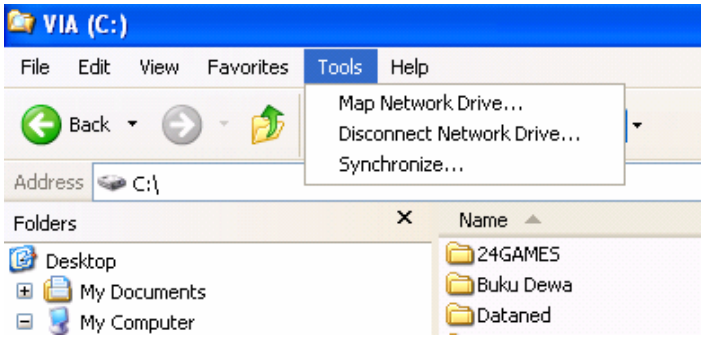
2. Pemblokiran Terhadap Msconfig (Microsoft Configuration)

Selain dari fasilitas *registry* yang diblokir, rontokbro pun akan memblokir fasilitas *msconfig*, yang merupakan utility untuk pengatur proses pemanggilan file apa saja yang akan dijalankan pada saat *startup*. Hal ini mungkin dilakukan untuk melindungi dirinya dari penonaktifan *loading* file pada saat *startup*, karena dari situlah sebuah proses pengembangbiakan rontokbro aktif. Hal ini dapat dibuktikan dengan mengetik msconfig pada menu run, atau menjalankan langsung dari explorer, maka secara otomatis computer akan restart.

3. Pemblokiran Terhadap CMD (Command)

File CMD atau Command yang kita kenal selama ini, merupakan fasilitas command prompt sebagai console turut diblokir pula, karena melalui ini pula kita dapat melakukan editing terhadap file autoexec.bat atau mengangkat status hidden file, menghapus secara manual dan lain sebagainya. Ini dapat dibuktikan dengan mengetik CMD atau Command pada menu run, atau menjalankan langsung dari explorer, maka secara otomatis computer akan restart.

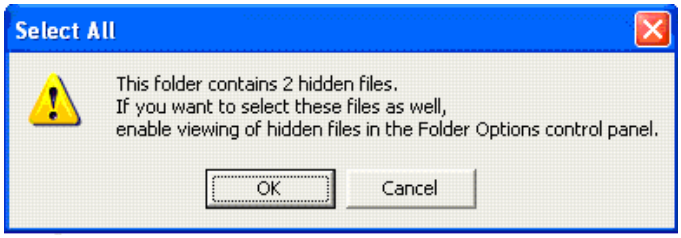
4. Pemblokiran Terhadap Fasilitas Folder Option



***Gambar 7** : Fasilits folder option tidak tampak pada windows explorer menu tools, disembunyikan sebagai bentuk perlindungan.*

Fasilits folder option pada menu Tool → Folder options di windows explorer yang biasa kita kenal untuk mengatur tampilan file pada windows explorer pun turut diblokir, hal ini dilakukan karena file-file virus rontokbro dibuat dengan status hidden file, dengan terlebih dahulu mengatur tampilan hanya untuk file yang bukan merupakan hidden dan system. Hal ini dapat dibuktikan dengan memilih menu tools pada windows explore, disana akan diketahui bahwa sub menu folder options yang selama ini ada menjadi hilang, sehingga kita tidak dapat menampilkan file-file hidden dan file system.

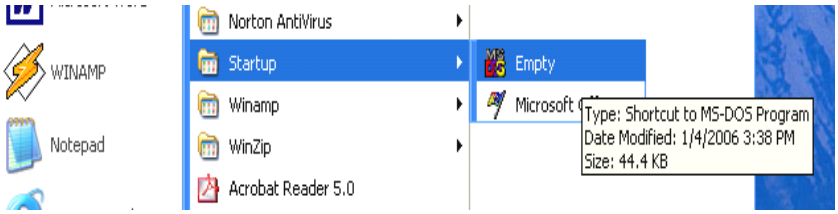
5. Penempatan File Empty.pif pada menu Startup Yang Tidak Terlihat



***Gambar 8** : File Rontokbro disembunyikan.*

File empty.pif yang diletakkan pada menu startup tidak akan kita sadari, karena file ini dibuat dalam bentuk hidden. Sehingga akan selalu dijalankan ketika system windows memasuki tahap logon.

6. Penempatan file-file tertentu pada direktori windows yang merupakan root directory system windows



***Gambar 9** : File empty.pif diletakkan di menu stratup untuk mengaktifkan setiapkali login.*

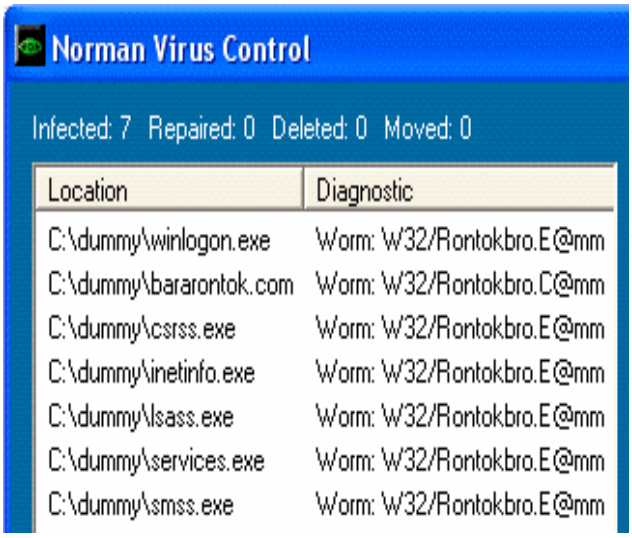
Adapun directory yang menjadi sasaran dari rontokbro adalah dengan melakukan pengkopian file terhadap system windows sebagai berikut :

%System%\[USER NAME]'s Setting.scr
%UserProfile%\APPDATA\IDTemplate.exe
%UserProfile%\APPDATA\services.exe
%UserProfile%\APPDATA\lsass.exe
%UserProfile%\APPDATA\inetinfo.exe
%UserProfile%\APPDATA\csrss.exe
%UserProfile%\Programs\Startup\Empty.pif
%UserProfile%\Templates\A.kotnorB.com

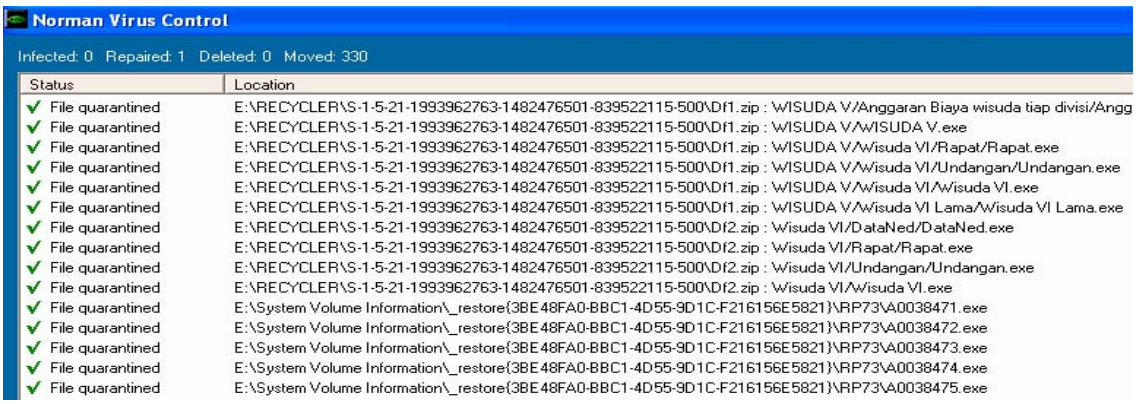
%System%\3D Animation.scr

Detail dari lokasi pengkopian :

\Windows\PIF\CVT.exe
\Windows\IDTemplate.exe
\Windows \eksplorasi.exe
\Windows\sempalong.exe
\Windows\ElnorB.exe
\Windows\bronstab.exe
\Windows\Brengkolang.com
\Windows\bararontok.com
\Windows\A.kotnorB.com
\Windows\WowTumpeh.com
\Windows\BronNetDomList.bat
\Windows\BronFoldNetDomList.txt
\Windows\BronNPath0.txt
\Windows\rontokbro.txt
\Windows\Kosong.Bron.Tok.txt



***Gambar 10** : Norman Virus Control mampu menangkap file-file rontokbro.*



***Gambar 11** : Norman virus control mampu membasmi file rontokbro*

\Windows\eksplorasi.pif
\Windows\Empty.pif
\Windows\3D Animation.scr
\Windows\ShellNew\eksplorasi.exe
\Windows\ShellNew\sempalong.exe
\Windows\ShellNew\IDTemplate.exe
\Windows\ShellNew\ElnorB.exe
\Windows\ShellNew\bronstab.exe
\Windows\ShellNew\Brengkolang.com
\Windows\ShellNew\bararontok.com
\Windows\ShellNew\A.kotnorB.com\Windows\ShellNew\WowTumpeh.com
\Windows\ShellNew\BronNetDomList.bat
\Windows\ShellNew\BronFoldNetDomList.txt
\Windows\ShellNew\BronNPath0.txt
\Windows\ShellNew\rontokbro.txt
\Windows\ShellNew\Kosong.Bron.Tok.txt
\Windows\ShellNew\eksplorasi.pif
\Windows\ShellNew\Empty.pif
\Windows\ShellNew\3D Animation.scr

Pengkopian file ke lokasi C s/d Y melalui alamat email dengan menggunakan file berekstension: .asp; .cfm; .csv; .doc; .eml; .html; .php; .txt; .wab

Catatan:
Lokasi penempatan pada filder system windows berbeda-beda tergantung dari versi windowsnya, sebagai berikut : \Windows\System (Windows 95/98/Me), \Winnt\System32 (Windows NT/2000), \Windows\System32 (Windows XP). \Documents and Settings\[CURRENT USER] (Windows NT/2000/XP).

7. Penambahan atau Perubahan Nilai-Nilai Tertentu Pada Registry

Untuk melakukan proses pemblokiran atas segala sesuatu yang akan membasmi dirinya, rontrokbro telah menambahkan atau merubah nilai-nilai tertentu pada registry, diantaranya adalah :

a. Menambahkan nilai DisableRegistryTools=1, diletakkan pada registry :
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
b. Menambahkan nilai DisableRegedit=1, diletakkan pada registry:
   HKCU\Software\Microsoft\Windows\CurrentVersion\Policies
c. Menambahkan nilai Disable CMD=1, diletakkan pada registry:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
d. Menambahkan nilai Bron-Spizaetus" = "C:\WINDOWS\PIF\CVT.exe atau Bron-Spizaetus" = ""%Windir%\ShellNew\sempalong.exe,diletakkan pada registry:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
e. Menambahkan nilai Tok-Cirrhatus" = "%UserProfile%\Local Settings\Application Data\smss.exe, diletakkan pada registry:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
f. Menambahkan nilai "Shell"="Explorer.exe"%Windir%\eksplorasi.exe"", diletakkan pada registry:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
g. Menambahkan nilai "Hidden" = "1","HideFileExt" = "1","ShowSuperHidden" = "0", diletakkan pada registry:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
h. Menambahkan nilai NoFolderOptions=dword:00000001, diletakkan pada registry:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

8. Pembuatan foler secara otomatis dan pemanipulasian file autoexec.bat

Pembuatan folder secara otomatis (variables [X]-[Y] dengan 2 nomor acak pada :

%UserProfile%\Local Settings\Application Data\Bron.tok-[X]-[Y]
%UserProfile%\Local Settings\Application Data\Bron.tok-24

Merubah isi dari file autoexec.bat dengan :
Menambahkan perintah "*pause*"

9. Penambahan Schedule Task

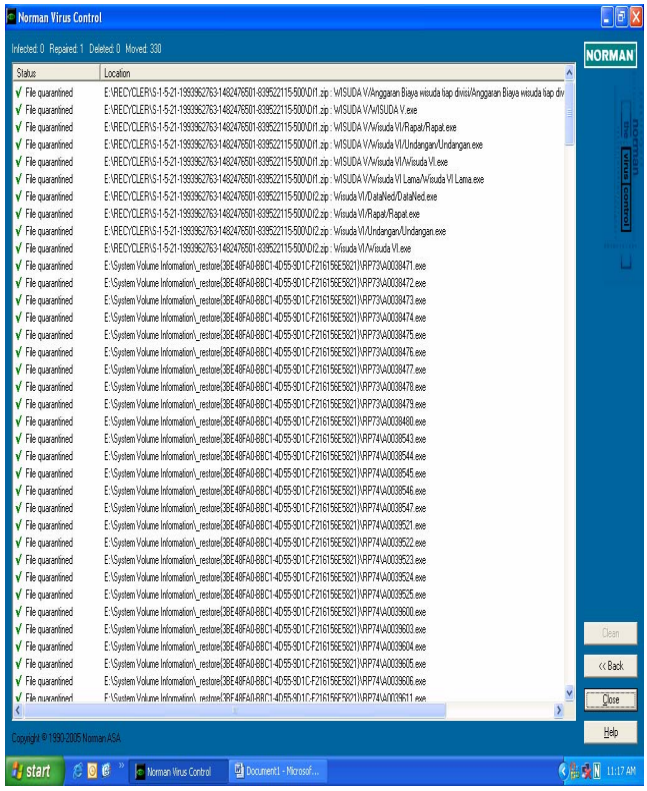
Sebagai aktivitas rutinnya yang dijalankan secara otomatis dalam pengembangbiakan dirinya, rontokbro telah membuat Schedule pada Schedule Task yang akan dijalankan setiap jam 5.08 PM, yaitu :

%UserProfile%\Templates\A.kotnorB.com
%UserProfile%\Templates\Brengkolang.com

10. Penambahan File Pada Menu Startup

Dalam menjalankan aktifitasnya, rontokbro telah menambahkan file *NorBtok*, *Smss*, *Empty* pada menu Startup, yang dijalankan secara otomatis melalui menu startup yang telah diconfigurasi pada msconfig.

Pemburuan Virus Rontokbro



***Gambar 12** : Pemburuan rontokbro yang dilakukan dengan Norman Virus Control*

Ketika penulis merasa, bahwa computer penulis tidak bekerja seperti biasanya, dimana windows berjalan dengan sangat lambat, hardisk selalu berkerja walaupun tidak ada aplikasi yang dibuka, lantas penulis melakukan scaning virus dengan fasilitas antivirus yang telah ada dikomputer penulis yaitu NORMAN. Namun demikian NORMAN mampu mendeteksi file-file yang dicurigai terinfeksi rontokbro maupun file virus itu sendiri. Norman berhasil melakukan clean, delete dan quarantine terhadap virus, namun demikian hal ini terbatas pada pembasmian sementara, sebab ketika windows direstart kembali rontrokbro kembali beraksi mengembangbiakan dirinya. Setiap harinya dalam waktu kurang dari satu jam, rontokbro berhasil mengembangbiakan dirinya hingga ± 400 file, dan jumlah ini akan terus bertambah, hingga suatu saat penulis membiarkan dalam sehari, sambil memperhatikan lampu indicator hardisk yang terus bekerja, hasilnya ketika penulis scan kembali berhasil mendeteksi ± 1000 file terinfeksi. Penulis juga melakukan scaning dengan MCAfee, hasilnyapun sama, MCAfee berhasil menemukan file–file manipulasi dari rontokbro.

Berikut adalah beberapa file rontokbro yang penulis temukan di computer penulis :

D:\WINDOWS\eksplorasi.exe
D:\WINDOWS\sempalong.exe
D:\WINDOWS\Brengkolang.com
D:\WINDOWS\IDTemplate.exe
D:\WINDOWS\bararontok.com
D:\WINDOWS\A.kotnorB.com
D:\WINDOWS\3D Animation.scr
D:\WINDOWS\ElnorB.exe
D:\WINDOWS\bronstab.exe
D:\WINDOWS\WowTumpeh.com
D:\WINDOWS\BronFoldNetDomList.txt
D:\WINDOWS\BronNetDomList.bat
D:\WINDOWS\BronNPath0.txt

D:\WINDOWS\rontokbro.txt
D:\WINDOWS\Kosong.Bron.Tok.txt
D:\WINDOWS\eksplorasi.pif
D:\WINDOWS\Empty.pif
D:\WINDOWS\ShellNew\eksplorasi.exe
D:\WINDOWS\ShellNew\sempalong.exe
D:\WINDOWS\ShellNew\Brengkolang.com
D:\WINDOWS\ShellNew\IDTemplate.exe
D:\WINDOWS\ShellNew\bararontok.com
D:\WINDOWS\ShellNew\A.kotnorB.com
D:\WINDOWS\ShellNew\3D Animation.scr
D:\WINDOWS\ShellNew\ElnorB.exe
D:\WINDOWS\ShellNew\bronstab.exe
D:\WINDOWS\ShellNew\WowTumpeh.com
D:\WINDOWS\ShellNew\BronFoldNetDomList.txt
D:\WINDOWS\ShellNew\BronNetDomList.bat
D:\WINDOWS\ShellNew\BronNPath0.txt
D:\WINDOWS\ShellNew\rontokbro.txt
D:\WINDOWS\ShellNew\Kosong.Bron.Tok.txt
D:\WINDOWS\ShellNew\eksplorasi.pif
D:\WINDOWS\ShellNew\Empty.pif

D:\Documents and Settings\Junaidi\Local Settings\Application Data\winlogon.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\services.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\lsass.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\inetinfo.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\csrss.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\smss.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\eksplorasi.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\sempalong.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\Brengkolang.com
D:\Documents and Settings\Junaidi\Local Settings\Application Data\IDTemplate.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\bararontok.com
D:\Documents and Settings\Junaidi\Local Settings\Application Data\A.kotnorB.com
D:\Documents and Settings\Junaidi\Local Settings\Application Data\3D Animation.scr
D:\Documents and Settings\Junaidi\Local Settings\Application Data\ElnorB.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\bronstab.exe
D:\Documents and Settings\Junaidi\Local Settings\Application Data\WowTumpeh.com
D:\Documents and Settings\Junaidi\Local Settings\Application Data\BronFoldNetDomList.txt
D:\Documents and Settings\Junaidi\Local Settings\Application Data\BronNetDomList.bat
D:\Documents and Settings\Junaidi\Local Settings\Application Data\BronNPath0.txt
D:\Documents and Settings\Junaidi\Local Settings\Application Data\rontokbro.txt
D:\Documents and Settings\Junaidi\Local Settings\Application Data\Kosong.Bron.Tok.txt
D:\Documents and Settings\Junaidi\Local Settings\Application Data\eksplorasi.pif
D:\Documents and Settings\Junaidi\Local Settings\Application Data\Empty.pif
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\eksplorasi.exe
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\sempalong.exe
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\Brengkolang.com
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\IDTemplate.exe
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\bararontok.com
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\A.kotnorB.com
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\3D Animation.scr
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\ElnorB.exe

D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\bronstab.exe
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\WowTumpeh.com
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\BronFoldNetDomList.txt
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\BronNetDomList.bat
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\BronNPath0.txt
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\rontokbro.txt
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\Kosong.Bron.Tok.txt
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\eksplorasi.pif
D:\Documents and Settings\Junaidi\Start Menu\Programs\Startup\Empty.pif
D:\Documents and Settings\Junaidi\Templates\eksplorasi.exe
D:\Documents and Settings\Junaidi\Templates\sempalong.exe
D:\Documents and Settings\Junaidi\Templates\Brengkolang.com
D:\Documents and Settings\Junaidi\Templates\IDTemplate.exe
D:\Documents and Settings\Junaidi\Templates\bararontok.com
D:\Documents and Settings\Junaidi\Templates\A.kotnorB.com
D:\Documents and Settings\Junaidi\Templates\3D Animation.scr
D:\Documents and Settings\Junaidi\Templates\ElnorB.exe
D:\Documents and Settings\Junaidi\Templates\bronstab.exe
D:\Documents and Settings\Junaidi\Templates\WowTumpeh.com
D:\Documents and Settings\Junaidi\Templates\BronFoldNetDomList.txt
D:\Documents and Settings\Junaidi\Templates\BronNetDomList.bat
D:\Documents and Settings\Junaidi\Templates\BronNPath0.txt
D:\Documents and Settings\Junaidi\Templates\rontokbro.txt
D:\Documents and Settings\Junaidi\Templates\Kosong.Bron.Tok.txt
D:\Documents and Settings\Junaidi\Templates\eksplorasi.pif
D:\Documents and Settings\Junaidi\Templates\Empty.pif

Dan masih banyak lagi, yang tidak dapat penulis tampilkan seluruhnya

Membasmi Virus Rontokbro

Pada pembahasan diatas, kita mencoba membasmi virus rontokbro dengan Norman, MCAfee, Norton hasilnya tetap sama, yaitu virus itu akan kembali beraksi ketika computer direstart, hal ini disebabkan karena rontorkbro telah menyerang bagian-bagian vital dan menempatkan file-file tertentu pada lokasi system dan startup serta registry. Melihat pengalaman ini, cobalah dengan versi terbaru dari Norman, MCAfee, Norton. Scanning ini sebaiknya dilakukan dengan windows dalam keadaan save mode. Dalam keadaan save mode ini dapat juga dilakukan dengan manual, jika kita memahami persis lokasi dari file-file rontokbro.

Jika scaning ini tidak berhasil juga, atau fasilitas save mode pun tidak bisa diakses, dapat juga dilakukan dengan system windows yang telah ada antivirusnya serta terbebas dari virus, letakkan hardisk yang bervirus sebagai slave bukan primary, dan hardisk yang berisi windows dan antivirus yang terbebas dari virus sebagai primary. Setelah hal ini berhasil, lakukan pencarian secari manual dengan fasilitas find untuk semua file dan folder berextention .exe, jika ditemukan, perhatikan file-file berekstention .exe atau application dengan lambang folder, file ini patut dicurigai sebagai rontrokbro, hapus saja tanpa ragu. Jika berhasil, kembalikan hardisk yang telah dibersihkan ke primary, dan jalankan kembali. Setelah berhasil memasuki windows cobalah lakukan editing registry melalui Start→Run→Regedit, dengan melakukan penghapusan pada lokasi berikut ini (Perhatikan penyerangan rontokbro pada pembahasan perlindungan diri virus rontokbro dan aktivitas penyerangannya) :

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\Bron-Spizaetus
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\Tok-Cirrhatus
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Policies\System\DisableRegistryTools
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Policies\System\DisableCMD
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Policies\Explorer\NoFolderOptions
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\advanced\Hidden
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\advanced\HideFileExt
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\advanced\ShowSuperHidden

Jika hal inipun tidak berhasil dilakukan, saran penulis lakukan instalasi ulang (Sebab virus rontokbro telah terlalu lama menyerang, dan sulit diperbaiki), dengan terlebih dahulu menyelamatkan data-data penting, lalu masukan antivirus versi terupdate seperti Norman, MCAfee, Norton. Jangan lakukan pembukaan file apapun sebelum dilakukan scanning dan pembasmian.

Pencegahan Virus Rontokbro

Selain control yang dilakukan oleh antivirus secara terus menerus untuk mencegah aktifitas virus, langkah pencegahan pun dapat dilakukan dengan berhati-hati dalam membuka file. Pada windows explorer selalu menampilkan fila dengan mode list atau detail. Dan perhatikan file dengan icon folder, jika berextention .exe atau application, hapus saja, jangan dibuka, karena jika sekali saja dibuka, maka rontokbro akan kembali bergerilia.

Penutup

Melihat dari pesan-pesan yang disampaikan virus rontokbro jelas ini berasal dari para hacker Indonesia. Disatu sisi kita berbangga dengan ini, karena para hacker Indonesia telah mampu menembus dunia Internasional. Tapi dilain sisi, kitapun merasa sangat terganggu karena aktivitasnya sangat menggangu kinerja computer.

Bagi penulis, pembuat virus rontokbro ini masihlah pemula, karena dari cara-cara penyebarannya mudah terdeteksi dan diketahui, misalnya saja aktivitasnya yang mengandalkan registry, menciptakan file mandiri bukan include pada file tertentu, penambahan kata pause pada autoexec.bat, penempatan file-file tertentu yang dapat diketahui ciri-cirinya, dan masih banyak lagi.

Kalau secara konsep, dan telah penulis praktekkan sendiri, virus rontokbro sangat mudah untuk dibasmi, misalnya saja dengan menggunakan bootable melalui floppy disk, atau CD. Lalu melakukan pengangkatan terhadap file hidden dengan fasilitas attrib pada dos, dilanjutkan dengan penghapusan file-file yang dicurigai pada lokasi-lokasi vital, serta pengeditan terhadap autoexe.bat, system.ini serta masih banyak lagi.

Pada akhirnya dalam senyum penulis mengatakan, ***"Rontokbro tidak ada apa-apanya, tujuan kalian tidak tercapai dalam menggangu aktifitas computer saya, karena saya merasa tertantang dengan semua itu, dan saya adalah sang pemburu, yang pada akhirnya saya pun mengetahui cara kerja kalian, hingga membasmi kalian dengan jejak yang kalian ciptakan atas kebodohan kalian sendiri"***.

Referensi

http://www.mcafee.com
http://www.norman.com

Biografi Penulis

Junaidi. Menyelesaikan S1 di Universitas Budi Luhur, Jakarta, tahun 2001. Sedang menjalani program pasca sarjana Magister Teknologi Informasi. Dosen di Sekolah Tinggi Manajemen Dan Ilmu Komputer, juga sebagai Kepala Jurusan Teknik Informatika, *System Analyst*, *Programmer* dan *Consultant*. Kompetensi inti pada bidang *Software Engineering*, *Database Design System*, *Database Design Concept*, dan *Konowledge Management*. Penulis aktif, dalam menulis artikel, tutorial dan jurnal yang telah diterbitkan di jurnal ilmiah. Aktif di beberapa organisasi kemahasiswaan, kelompok studi ilmiah, kelompok belajar dan dewan penasehat himpunan mahasiswa jurusan sistem informasi.