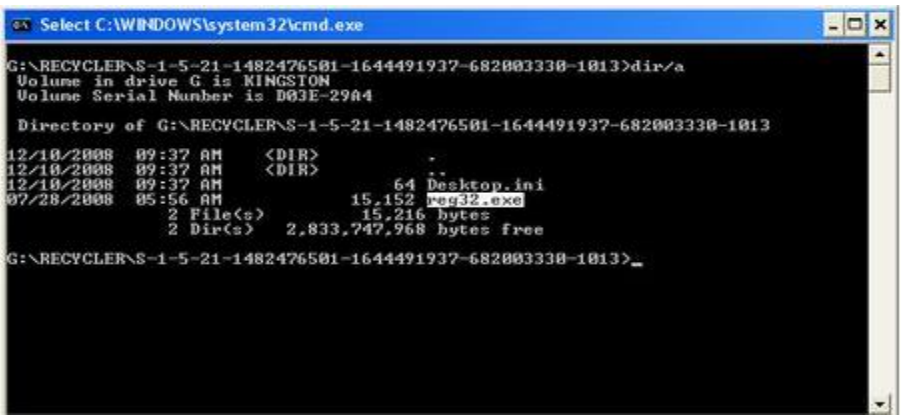
Virus bandel manfaatkan Tempat Sampah

Anharku
v_maker@yahoo.com
http://anharku.freevar.com

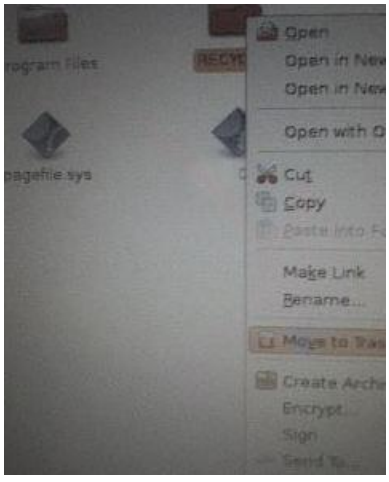
Pernah ga mengalami instal ulang berkali-kali namun virus masih saja ga ilang-ilang? Lalu kamu bertanya loh? Kok bias kena-kena lagi yah?? Lalu kamu berpikir…apa da virus yang g sengaja masuk waktu aku instal-instal program?? Coba2 diurut satu persatu instal ini itu normal baru setelah buka drive yang lain JBRET….. AGH..TIDAKKKK…. task manager tertutup, registry editor ga bisa dibuka..ampun dagh berarti.. Langsung mengambil kesimpulan ini adalah virus yang menyebar dengan teknik buka Drive.. Jadi sekalipun kamu instal ulang ratusan kali virus akan mencemari drive System saat kamu membuka Drive lain yang berada pada computer tersebut. Kok bias gitu? Lalu dimana virus bersarang? Jadi penasaran Munculkan dulu semua file hidennya **Tool-FolderOptions-View-Show Hiden files and folders, hilangkan ceklist pada hide protected operating system file(Recommendet)** lalu lihat Drive nya? Wah2 aman2 aja ga ada file .exe yang mencurigakan g ada autorun.inf?? dimana?? Tempat sampah (Folder Recycler).

Nah disinilah sebenarnya sarang dari persembunyian virus namun untuk mengetahuinya kita harus menjelajah lebih dalam dengan perintah dari Command Prompt ketik di cmd misalnya menengok drive G ketik G: (enter) lau ketik CD RECYCLER(enter) lalu ketik CD S-1-5-21-1482476501-1644491937-682003330-1013(enter) kemudian ketik **dir /a.**



Nah2.. terlihat sudah virus yang bikin BT karena install ulang berkali-kali. Ini adalah virus **Recycler**. Sampai saat ditulis tutorial ini virus ini memiliki beberpa varian Recycler.J, K, dan L,kemudian varian Recycler.M, N, O, dan P. virus ini menyamar seperti layaknya Recycle Bin. Contohnya disaat virus ini menyerang flash disk. Di flash disk korban akan terdapat folder dengan nama Recycler yang di dalamnya terdapat folder yang menggunakan nama *alpha numeric* contohnya "S-1-5-21-1482476501-1644491937-682003330-1013" dan di dalamnya terdapat file virus bernama reg32.exe. Lalu mengapa bisa berjalan hanya dengan membuka Drive?? Ternyata virus ini Ia menerapkan teknik *code injection* agar kode virus bisa "nyangkut" pada explorer.exe jadi saat kamu membuka drive=menjalankan explorer.exe=menjalankan virus ☹. Coba2.. delete folder RECYCLER dulu…

Yah Error nih g bisa di delete.. penyebabnya apa? **Disk is not full or write-protected, the file is not currently in use**..(boso opo kui)intinya akses penghapusan ditolak windows melakukan perlindungan terhadap folder tersebut. Haduh2 sekarang solusinya gimana Bro aku udah setengah mati instal terus… Masak aku harus format semua Driveku?? Nanti data pentingku… Data sekolahku… Source Codeku.. foto pacarku.. *Vidio kesukaanku (Vidio penyebab kena musibah ☺)*.



Jangan dulu bro masih ada satu jalan pernah denger Booting dengan CD Live Linux? Kenapa linux? Karena linux bisa membaca file-file windows. Masuk ke **BIOS** ganti bagian **First Boot Device ke CDROM**. Masukkan cd booting Linuxnya lalu masuk ke tampilan muka linux buka **Document**, buka Drive kamu.. dan Klik folder RECYCLER –**Move To Trash**..kok bisa dihapus? Dasar aneh yah bisalah kan Beda OS…ya bisa dunk ☺ lakukan juga penghapusan folder RECYCLER yang terdapat pada Drive-drive lainnya…pokoknya sampe bersih…Jika kamu tidak dapat mengakses Drive system kamu misal **21.0 GB Media** tidak dapat diakses dari linux usahakan kamu menghapus folder RECYCLER yang terdapat pada drive lain yang terdapat pada komputermu, lalu instal ulang Drive System kamu (instal ulang Drive C).

Banyak virus yang memanfaatkan baik folder RECYCLER (tempat sampah) maupun System Volume Information sebagai tempat persembunyianya. Contoh virusnya yah: **virus Recycler variant, virus recycled, virus Autorunme variant, dll** Yang g mungkin saya sebutkan semua disini.. .

Semoga yang dikit ini bisa membantu..

Biografi Penulis

Anharku. *Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan,merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet sejak hobi main di warnet untuk sekedarmengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart,dan belajar bahasa pemrogramanseperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL,belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.*