

## VIRUS & INTERNET

Anharku

v\_maker@yahoo.com

<http://anharku.freevar.com>

Lisensi Dokumen:

Copyright © 2003-2009 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

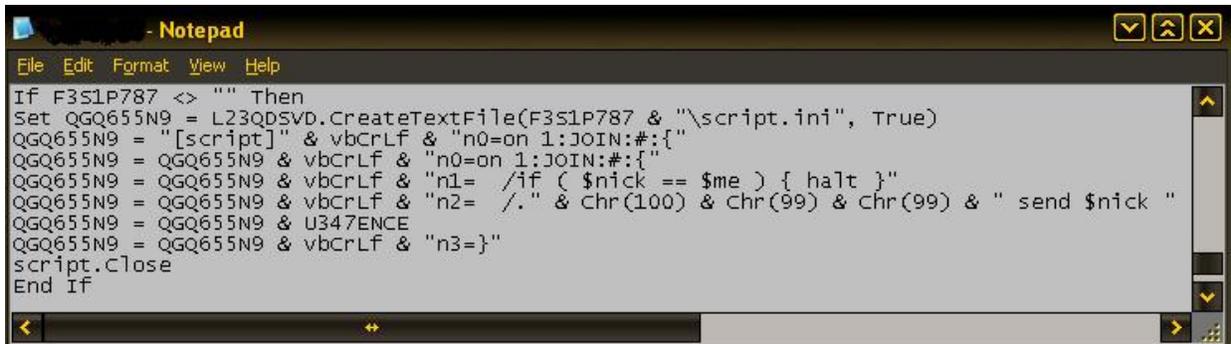
**K**lo membicarakan tentang virus pasti kita juga akan membicarakan internet, Mengapa? Karena kebanyakan virus yang telah beradaptasi dengan dunia menggunakan internet sebagai media penyebarannya, tidak hanya menggunakan media penyebaran floppy atau flashdisk seperti yang telah dilakukan pada virus-virus lokal kebanyakan.

Banyak virus yang menyebarkan dirinya lewat internet misalnya: **W32/Emmareg.A** yang mencoba menyebar melalui email dengan mengirimkan [reply] semua email yang ada di INBOX dengan menyertakan attachment NOVA.SCR. **W32/VB Worm.MLG** yang memalsukan diri sebagai PCMAV antivirus RC9 meminta kita untuk percaya dan mendownload virus tersebut. **W32/Viking.GU** yang mengakibatkan traffic jaringan menjadi padat hal ini dikarenakan Viking mencoba untuk melakukan ping request dengan melakukan scan terhadap semua IP yang terdapat dalam subnet lokal yang ada di dalam jaringan tersebut hal ini ditambah lagi dengan aksi lainnya dengan mencoba untuk mengkopikan dirinya ke komputer target serta menginfeksi file yang mempunyai ekstensi EXE.

Baru-baru ini saja ada virus **Anjelina Jolie(W32/Agent.GPKB)** yang mengirimkan e-mail berisi tawaran untuk memperoleh video syur FREE alias Gratis dengan embel-embel seakan-akan email tersebut merupakan Fitur dari Microsoft MSN. Lalu versi ke 2 dari virus Anjelina Jolie ini yaitu **Anjelina Jolie II (W32/DLoader.ITOA)** yang akan memalsukan isi berita dari CNN dan MSNBC. Virus ini dikategorikan sebagai Spyware dan mempunyai ciri-ciri yang tidak jauh dengan pendahulunya (Agent.GPKB), virus ini juga akan men-download sebuah program lain sama seperti pendahulunya yakni antivirus XP 2008 yang secara otomatis akan langsung di install di komputer korban. **Anjelina Jolie II** ini menyebarkan email dari Daily Top 10 dengan

subject CNN.com Daily Top 10, harap berhati-hati apalagi jika diminta untuk download sebuah file dengan nama get\_flash\_update.exe pada saat anda klik salah satu berita dalam bentuk video yang di sertakan pada email tersebut.

Saat saya lagi main-main ke warnet untuk mencari suasana sambil memandangi kecantikan penjaga warnetnya ☺ ternyata saya pulang dengan membawa oleh-oleh sebuah file.vbs yang berisi kode-kode untuk menggandakan diri dan menyebarkan dirinya melalui internet koding penyebaran internetnya dapat dilihat pada gambar berikut:



```
IF F3S1P787 <> "" Then
Set QQ655N9 = L23QDSVD.CreateTextFile(F3S1P787 & "\\script.ini", True)
QQ655N9 = "[script]" & vbCrLf & "n0=on 1:JOIN:#{
QQ655N9 = QQ655N9 & vbCrLf & "n0=on 1:JOIN:#{
QQ655N9 = QQ655N9 & vbCrLf & "n1= /if ( $nick == $me ) { halt }"
QQ655N9 = QQ655N9 & vbCrLf & "n2= /." & Chr(100) & Chr(99) & " send $nick "
QQ655N9 = QQ655N9 & U347ENCE
QQ655N9 = QQ655N9 & vbCrLf & "n3=}"
script.close
End If
```

Dari kode diatas dapat saya tarik kesimpulan bahwa virus ini akan membuat suatu file bernama script.ini yang berfungsi memasuki channel yang telah diketahui dan mengirimkan nick berupa nama dari virus tersebut. Kode tersebut sangat terlihat bahwa virus ini menyebarkan diri lewat internet (khususnya IRC).

Mengapa memilih IRC sebagai media penyebarannya? Karena IRC memiliki kelebihan penulisan perintah-perintah DCC. File tersebut di set secara automatic sehingga virus tersebut dapat diantar melalui DCC.

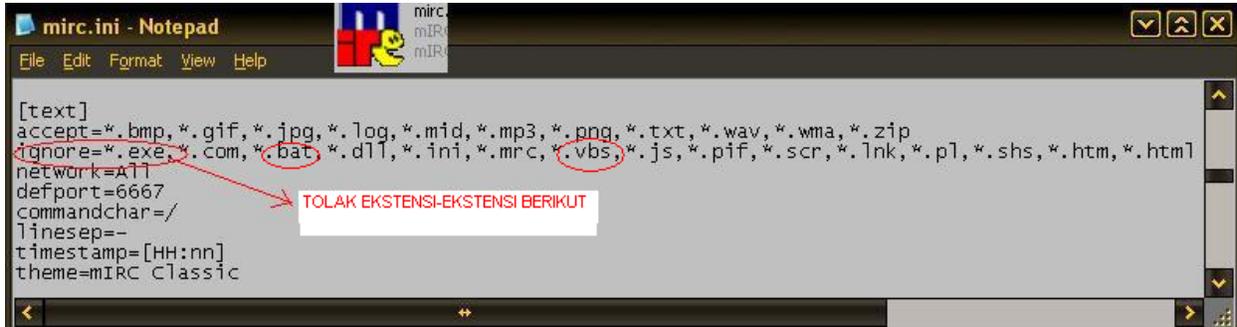
IRC mempunyai sistem untuk menerima atau menolak file yaitu dengan menuliskan perintah /dccallow +nama pengantar, yang akan membenarkan anda menerima file itu. Oleh karena penyebaran virus tiap- tiap hari di DALnet, DALnet mempunyai satu fungsi yang membatasi penghantaran DCC bagi fail dengan koneksi ("js", "pl", "exe", "com", "bat", "dll", "ini", "vbs", "pif", "mrc", "scr", "doc", "xls", "lnk", "shs", "htm", "html"). Untuk mendapatkan file tersebut, Unit Kod DALnet telah menambahkan perintah DCCallow. Perintah DCCallow ,yaitu dengan menuliskan

Syntax: /quote dccallow +/-nickname, Informasi: +/-nama\_samaran mesti dinyatakan untuk anda menyatakan siapa yang anda izinkan menghantar DCC kepada anda. Jadi anda dapat menentukan sendiri orang-orang yang anda percaya dalam mengirimkan file.

Jika anda menggunakan IRC, Kerap kali anda akan mengalami masalah pengguna IRC yang mencoba menghantar file virus dan trojan. File- file tersebut misalnya Movie.avi.pif, Links.vbs dll. Ada juga file berupa 'backdoors'. Jika file tersebut dipanggil, ia bisa memberi laluan tanpa

izin kepada pengguna yang tidak bertanggung jawab untuk meng-exploit dan dan merusak komputer anda.

Anda hanya bisa mengatasi masalah ini dengan menetapkan opsi DCC anda kepada 'ignore'.

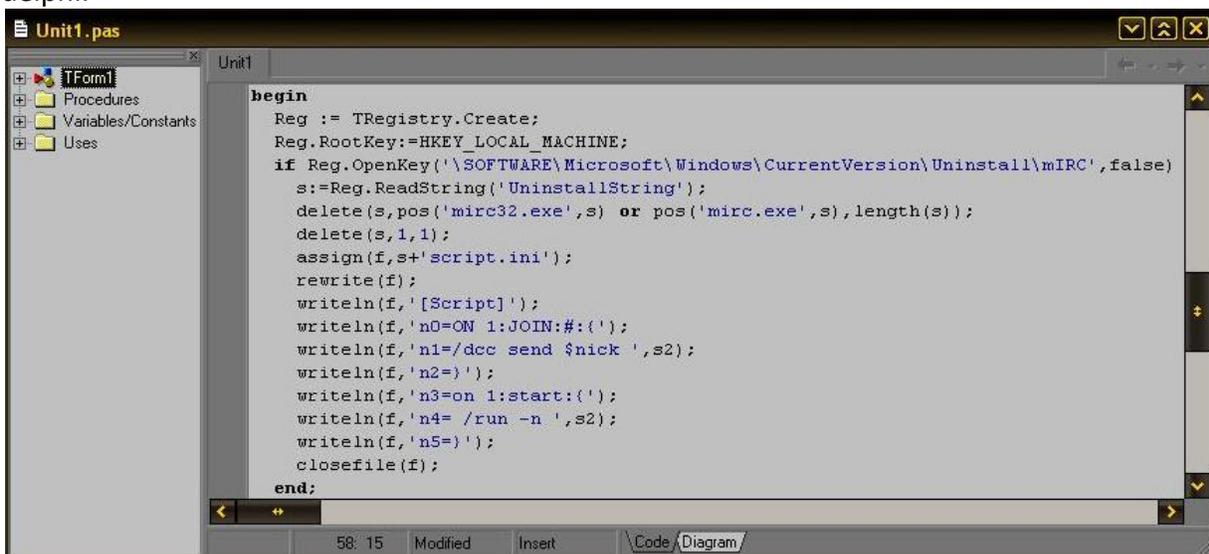


Dengan melihat file **mirc.ini** yang berisi daftar file yang diterima(lolos) ataupun yang ditolak(tidak diloloskan) seorang virus\_maker(vm) yang biasa mencari celah-celah keamanan pun dapat membuat duplikat dari file ini dengan menambah daftar file yang diterima(lolos) dengan ekstensi-ekstensi virus buatannya misal dalam daftar **accept** ditambah dengan **\*.exe,\*.vbs**

Sehingga serangan dari virus\_maker akan berjalan jauh lebih lancar dengan dibukanya celah tersebut ☺

Dan saran dari ku buat pengguna IRC, Jangan terima fail DCC dari orang yang tidak anda kenal, karna orang yang tidak anda kenal, atau tidak anda percaya tersebut bisa saja memberikan file berisi virus atau trojan.

Seperti tidak mau kalah rieysha juga membuat virus yang berjalan di IRC virus ini di buat dengan delphi.



Intinya sama dengan virus .vbs diawal yaitu virus akan membuat suatu file bernama script.ini yang berfungsi memasuki channel yang telah diketahui dan mengirimkan nick berupa nama dari virus tersebut dan menjalankan file virus tersebut (perintah run)

**Sekali lagi saya ingatkan virus hanyalah program biasa buatan manusia biasa, dengan selalu berhati-hati dan melakukan pencegahan-pencegahan anda yang jauh lebih pintar pasti tidak akan gentar menghadapinya hehehehe...☺**

### 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 sekedar mengecek 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.