

Hadapi virus alman dengan Cmd

Anharku

v_maker@yahoo.com

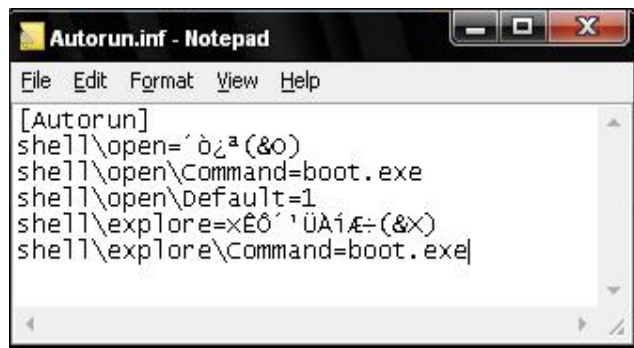
http://anharku.freevar.com

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.

Bagaimana virus Alman itu menyebar melalui autorun? Alman memanfaatkan autorun sebagai media penyebaran dengan memanipulasi file autorun.inf pada USB flashdisk sebagai berikut:



```
-----[scriptnya]-----  
[Autorun]  
shell\open=^ò¿^a(&O)  
shell\open\Command=boot.exe  
shell\open\Default=1  
shell\explore=×ÊÔ´¹ÜÀíÆ÷(&X)  
shell\explore\Command=boot.exe  
-----[end script]-----
```

Dari script diatas dapat dipelajari, Ketika autorun komputer berjalan maka induk virus dari virus alman ini akan dieksekusi atau dijalankan yang berarti virus alman akan mencemari komputer, karena autorun telah dimanipulasi oleh virus:

shell\open=^ò¿^a(&O) ---→buka ^ò¿^a(&O)

^ò¿^a(&O) = Open pada Removable Disk telah dimanipulasi oleh virus alman

Lalu:

1

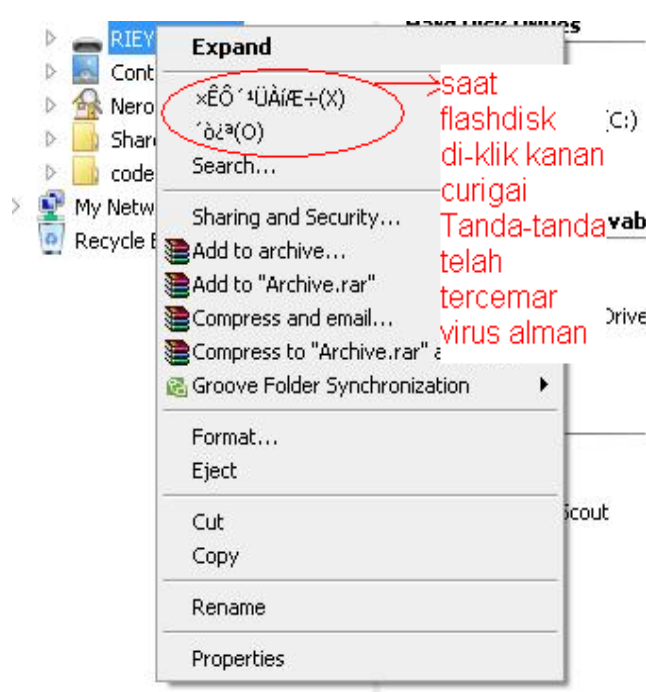
Komunitas eLearning IlmuKomputer.Com

Copyright © 2003-2009 IlmuKomputer.Com

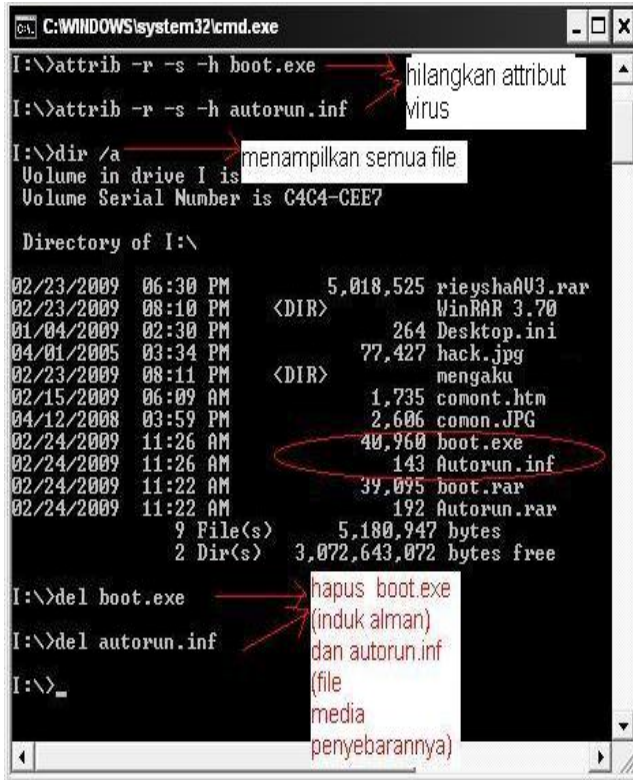
shell\open\Command=boot.exe->perintah untuk menjalankan induk virus alman (boot.exe)

Perintah ini yang membuat flashdisk menjadi terinfeksi virus alman tersebut,yang selanjutnya,jika komputer dicolokkan flashdisk ini dan autorun komputer jalan maka komputer tersebut menjadi terinfeksi virus alman.begitu dan seterusnya menyebar ke flashdisk2 yang di-share dengan komputer terinfeksi virus alman tersebut.

Sebenarnya kita dapat melihat kode special yang melekat pada tubuh virus maupun file yang telah di cemarinya kode tersebut adalah: **J6vÜ0fc** dan **16ä0øcc** (kata mas Hirin loh) sebenarnya kita juga dapat membuat aplikasi yang dapat mengidentifikasi apakah file aplikasi tersebut telah terinfeksi oleh virus alman.



Nah setelah beberapa penjelasan diatas sebaiknya saat membuka flashdisk kita lihat dahulu apakah flashdisk tersebut telah tercemar klik kanan pada Drive flashdisk tersebut jika seperti gambar berikut berarti flashdisk tersebut telah tercemar virus alman.



Jika di dalam flashdisk terdapat penyusup seperti ini jangan di buka dulu...entar nyebar lagi hikz..mau aplikasi2mu tercemar? Mau tool hacking-mu tercemar? Mau antivir-mu tercemar ga kan?? Next lakukan langkah berikut buka **Command Prompt** atau run-cmd lalu hilangkan attribut dari virus tersebut dengan mengetikkan perintah **attrib -r -s -h boot.exe**

- : menghilangkan attribute
- r : mengubah attribute file menjadi Read Only
- s : Mengubah attribute menjadi system
- h : mengubah attribute menjadi hidden.

Ketikkan **dir /a** untuk menampilkan semua file dalam flashdisk lalu delete induk virus alman dengan menuliskan perintah **del boot.exe**, hapus juga file penyebarannya yaitu **autorun.inf**

Dah dulu ya yang sedikit ini semoga 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.