VIRUS CONFLICKER

Latar Belakang Virus Conflicker

Virus conflicker merupakan virus jaringan dimana virus tersebut menyerang koneksi jaringan computer di tiap-tiap client computer yang terhubung jaringan sehingga komunikasi antar jaringan menjadi terganggu akibat virus tersebut Virus Conflicker menyebar pada bulan Oktober 2008. Pada tanggal 6 Januari 2009, New York Times memberitakan bahwa sekitar 9 juta PC di dunia telah terinfeksi virus conflicker (sumber: en.wikipedia.org).

Gejala-gejala yang ditumbulkan oleh virus conflicker

Gejala-gejala yang ditumbulkan oleh virus conflicker diantaranya adalah:

- Komunikasi jaringan computer terhambat
- Username Login di Active Directory (AD) Windows terkunci berulang-ulang
- Komputer mendapatkan pesan error Generic Host Process.
- Komputer tidak bisa mengakses situs-situs tertentu seperti www.microsoft.com, www.symantec.com, www.norman.com, www.clamav.com, www.grisoft.com, www.avast.com dan www.eset.com dengan pesan “Address not Found” tetapi jika situs-situs tersebut di akses dari alamat IPnya akan bisa diakses. Dan situs-situs lain tidak ada gangguan berarti.
- Update definisi antivirus terganggu karena akses ke situs antivirus diblok
- Banyak aplikasi tidak berfungsi dengan baik. Khususnya aplikasi yang memanfaatkan jaringan dan menggunakan port 445, 1024 s/d port 10.000.

Penanggulangan Virus Conflicker

Ada beberapa cara dalam penanggulangan virus conflicker yaitu :

- Putuskan koneksi jaringan antar computer untuk mencegah virus tersebut dapat menyerang computer lainnya (copot kabel jaringan)
- Backup semua data yang ada di drive C ke drive lainnya
- Unninstall semua antivirus yang terinstall di computer
- Non aktifkan semua services starup, dengan cara jalankan run pada start menu lalu ketikan msconfig > enter, sorot pada menu startup, hilangkan semua checklist lalu apply

- Restart computer setelah itu aktifkan computer pada mode safe mode, masuk pada login administrator
- Jalankan removal conflicker, disini saya menggunakan combofix
- Restart kembali computer setelah itu jalankan computer pada mode normal
- Check system dengan cara mengaktifkan show hidden file
- Jangan pernah mengklik drive lain selain drive c, itu mencegah virus yang ada pada drive lainnya masuk pada drive C (system)
- Masuk pada drive C, setelah itu check pada drive tersebut apakah ada file yang aneh di delete
- Masih pada drive C, sorot pada folder system volume informations lalu klik. Jika folder tersebut tidak bisa di klik, non aktifkan use simple file sharring di folder options dengan cara menghilangkan checklist tersebut lalu OK, setelah itu klik kanan mouse pada folder system volume informations lalu pilih properties > security > advanced > permissions > checklist ***"inherit from parent the permission sthat apply to child object"*** > apply > OK
- Setalah itu masuk kembali pada folder system volume information, lalu masuk pada semua folder _restore (ADA36B8F-9696-48A4-8988-E4A756986CC1) > check semua folder RP1, RP2 dst. Delete semua file yang ada difolder-folder tersebut
- Kembali pada lokasi drive C, lalu sorot folder $Recycle.Bin, Empty semua di recycle bin tersebut
- Setelah itu Disk cleanup drive tersebut di properties drive.
- Restart kembali computer, setelah itu jalankan mode computer pada mode safe mood
- Jalankan patching windows setelah itu restart kembali
- Jalankan computer pada mode normal, lalu install antivirus, setelah itu update antivirus
- Scan semua drive computer menggunakan antivirus sampai finish
- Restart computer
- Sambungkan kembali kabel jaringan
- Finish

Penanggulangan virus conflicker diusahakan serentak semua menanggulangi virus tersebut dikarenakan virus tersebut sangat cepat menyebar pada computer lainnya, conflicker selalu mencari celah untuk bisa menyebar kembali pada sebuah jaringan computer.

Terimakasih

Salam, Puskom FT UI