Memahami Kuda Troya Back Orifice dan Cara Menghalaunya

ÇäkrabiRâwÄ
Depok – Indonesia
Cakrabirawa@mail.ru
http://come.to/digitalworks

Tulisan ini pernah dimuat di Tabloid PCplus No. 90 – 91 Th. III/Agustus 2002

Back Orifice atau biasa disebut BO pada dasarnya merupakan program remote administrator yang digunakan oleh para administrator jaringan untuk mengontrol komputer lain yang saling berjauhan dalam satu jaringan. Hal ini tentunya akan sangat membantu tugas – tugas kesehariannya sebagai admininstrator jaringan. "Teknologi bersifat netral". Mungkin ada benarnya perkataan ini. Dan pada perkembangannya program tersebut disalahgunakan oleh orang yang tidak bertanggung jawab yang berotak nakal dan difungsikan sebagai trojan. "Orang memberi jiwa terhadap teknologi".

Pembuat BO

Back Orifice dibuat oleh sebuah gang komputer yang mengaku bernama "Cult of the Dead Cow" yang juga dikenal dengan singkatan CDC. Pada bulan Agustus 1998 mereka melepas Back Orifice ini ke Internet, memungkinkan siapa saja untuk men – download – nya dan membuka jalan bagi orang lain untuk mengambil alih kontrol komputer seseorang secara total tanpa sepengetahuan orang tersebut.

Paket BO

Paket Back Orifice sendiri pada intinya terdiri dari dua bagian, yaitu bagian client dan server. Bagian client – nya berupa file aplikasi BOGUI.exe yang berbasis Windows dengan tampilan GUI yang selalu berubah – ubah. Aplikasi yang berukuran sekitar 278 kb ini dipergunakan untuk mengontrol server. Perintah yang dapat dilakukan dengan aplikasi client BO terhadap server – nya cukup banyak, bahkan boleh dibilang hampir semua operasi yang dapat dilakukan oleh seorang user terhadap komputer di depannya dapat juga dilakukan oleh program BO ini. Kesemuanya mencapai lebih dari 50 perintah yang membentang dari TCP file send, HTTP disable, operasi file, memodifikasi registry Windows dan bahkan sampai menangkap tampilan layar monitor!

Gambar 1
Tampilan Back Orifice Client

Bagian server – nya hanyalah sebuah file yang bernama Boserve.exe. Tanpa icon. Begitu program ini dijalankan pada komputer yang akan dijadikan sebagai server, file BoServe.exe ini akan menghapus diri dan meng – copy dirinya ke direktori Windows\System menjadi file ".exe" (titik exe), yaitu sebuah file tanpa nama dengan ekstensi EXE. Tentu saja bila *setting* Folder Options Anda adalah "Hide file extensions for known file types", maka file ini akan tampak kosong saja. Satu teknik bersembunyi yang cukup handal.

Tidak cuma meng – copy dirinya ke folder System. Trojan ini juga memodifikasi sistem Windows yaitu registry. Akibatnya dia akan selalu aktif setiap kali Anda menghidupkan komputer. Registry yang dimodifikasi adalah pada cabang key Hkey_Local_Machine \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices. Hanya saja trojan ini tergolong masih "moderate" dibanding trojan SubSeven yang memodifikasi empat bagian di sistem untuk dapat aktif setiap kali Windows dijalankan, yaitu dengan mengubah 2 bagian di registry, satu di file WIN.INI dan satu lagi di file SYSTEM.INI. Sehingga bila hanya satu bagian sistem yang diperbaiki maka bagian lain akan tetap berfungsi dengan baik untuk menjalankan SubSeven.

Bagaimana Masuk ke Sistem

Yang harus Anda waspadai dari paket Back Orifice ini adalah file BoServe.exe. Tanpa file yang berukuran sekitar 122 kb ini Back Orifice tidak ada apa – apanya. File ini bisa saja disusupkan oleh orang – orang yang berniat jelek terhadap komputer Anda dengan berbagai cara termasuk menggunakan trik – trik yang menipu. Diantaranya adalah dengan mengirim suatu paket program yang nampaknya menarik tetapi di dalamnya memuat file BoServe.exe yang bisa jadi sudah diganti namanya menjadi yang lain, sehingga mengundang rasa penasaran orang untuk meng – klik – nya. Atau bisa juga dipaket dengan program – program gratisan atau bajakan yang dalam proses instalasinya memaksa untuk mengeksekusi file BoServe.exe. File ini bisa jadi telah diubah namanya sebagai bagian dari kamuflase dan memperlancar trojan BO untuk memasuki sistem Anda. Layaknya jalan tol yang bebas hambatan. Maka dari itu penulis menyarankan agar berhati – hati dalam menerima paket program dari sumber – sumber yang tidak dapat dipercaya.

Menaklukkan Kuda Jenis Ini

Untuk menaklukkan trojan ini Anda hanya perlu mengembalikan setting registry yang telah berubah tersebut dan menghapus file yang ada kaitannya dengan trojan BO. Berikut ini penulis beberkan cara menghalau kuda troya ini secara manual. Anda simak baik – baik langkah – langkahnya.

1. Jalankan Regedit dengan memilih menu START kemudian Run. Pada kotak yang kosong isikan Regedit. Tekan tombol OK sehingga jendela Regedit tampil memenuhi layar monitor
2. Buka key registry Hkey_Local_Machine \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices. Anda dapat mengklik tiap – tiap key untuk melihat sub key di bawahnya. Tampilan Registry Editor dengan bagian registry yang diubah oleh BO terlihat seperti pada gambar 3.
3. Sorot kata (Default) yang memuat data ".exe". Bagian inilah pemicu yang secara otomatis menjalankan trojan BO.
4. Kemudian pilih menu Edit > Delete. Pada konfirmasi yang ada tekan tombol Yes.
5. Tutup Regedit dan reboot komputer Anda.

Dengan langkah – langkah di atas Anda telah mengembalikan setting registry ke kondisi awal sebelum diacak – acak oleh trojan BO sekaligus mematahkan pemicunya yang memaksa Windows untuk menjalankannya secara otomatis bersamaan dengan dimulainya Windows. Tugas Anda belum selesai. Lanjutkan perburuan Anda dengan langkah selanjutnya ini.

1. Setelah proses booting selesai dan dimulai lagi sesi Windows, jalankan Windows Explorer dan buka folder Windows\System.
2. Carilah file ".exe" pada folder System itu. Ingat file tersebut tidak mempunyai icon dan nama file tetapi berekstensi exe dengan ukuran sekitar 122 kb. Gambarannya akan tampak seperti diperlihatkan pada gambar 2. Setelah ketemu, bunuh hasil buruan Anda tersebut dengan menekan tombol "Delete".

3. Masih pada direktori yang sama, buru juga file "windll.dll". File ini merupakan sebuah file yang dibuat oleh BO untuk mendukung operasinya.
4. Tutup semua aplikasi dan reboot kembali komputer Anda.

Akhirnya kuda troya dari "spesies" Back Orifice telah Anda taklukkan. Penulis sarankan untuk tetap terus memantau bagian registry di atas. Termasuk di dalamnya adalah bagian key Run, RunOnce, RunOnceEx, RunServices, dan RunServicesOnce. Karena bagian tersebut berfungsi menjalankan aplikasi secara otomatis saat komputer memulai Windows – nya. Banyak yang memanfaatkan key – key registry tersebut termasuk Windows sendiri dan juga program – program anti virus untuk mengaktifkan sistem proteksi komputer secara otomatis. Termasuk juga ditunggangi oleh banyak trojan. Hanya saja key registry ini tidak akan aktif saat Anda booting ke modus "Safe Mode". Tetapi siapa yang tahan terus – menerus menggunakan Windows dengan modus "Safe Mode".

Demikian sekelumit pembahasan mengenai trojan Back Orifice ini. Semoga Anda memahami cara kerjanya untuk dapat lebih lihai dalam menghalau trojan ini. Dan tetaplah terus mempelajari apa dan bagaimana trojan, virus dan program – program yang merusak lainnya, karena pengetahuan adalah ***the most basic*** dalam membentengi komputer dari serangan trojan dan kawan – kawannya.