Pelajaran dari Kasus Onel de Guzman: Telaah Kolaborasi antara Worm I Love You dengan Trojan Barok

Oleh : Happy Chandraleka

ABSTRACT

Many applications belong to malicious software, such as virus, worm, Trojan horse, Trojan mule, email bomb, and malicious script. However, the prominent ones are virus, worm, and Trojan horse. Each of these software bears different characteristics and manner. Most malicious software attacks are individual ones. Integrated attacks, collaboration between one malicious software with another, seldom happen. This article describes collaboration between I Love You worm with Trojan Barok, both of which are made by Onel de Guzman, a student from Manila.

Ada banyak perangkat yang dapat dikelompokkan ke dalam malicious software. Yaitu virus, worm, trojan horse, trojan mule, email bomb, dan malicious script. Tetapi yang paling utama adalah virus, worm, dan trojan horse. Masing-masingnya mempunyai karakteristik dan cara kerja yang berbeda-beda. Bila kita perhatikan, kebanyakan serangan malicious software bersifat individual. Sangat jarang terjadi serangan yang bersifat terpadu kolaborasi antara satu malicious software dangan malicious software yang lain. Pada tulisan ini dijelaskan kolaborasi antara worm I Love You dengan trojan Barok. Kedua malicious software ini dibuat oleh mahasiswa Manila yang bernama Onel de Guzman.

I. PENDAHULUAN

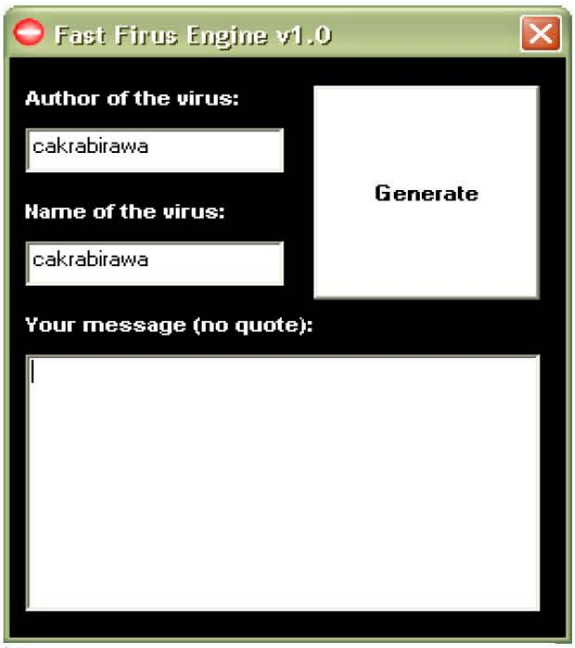
Menurut David Ferbrache dan Stuart Mort dalam Malicious Software and Hacking, malicious software diartikan sebagai sebuah software yang ditulis untuk menjalankan aksi yang tidak diinginkan oleh pengguna komputer. Aksi ini bisa bersifat pasif yang tidak merusak seperti menampilkan kotak pesan yang tidak berbahasa pada layar monitor, atau aksi-aksi yang agresif, seperti memformat harddisk.

Untuk membuat malicious software seseorang harus mengerti pemrograman. Tidak diperlukan level pemrograman yang tinggi dalam hal ini. Seseorang tidak harus menjadi orang yang jenius untuk membuat malicious software. Terlebih lagi dengan banyaknya situs-situs pemrograman di Internet yang menyediakan kode sumber dalam bentuk tips dan trik pemrograman.

Pada perkembangan berikutnya untuk menghasilkan sebuah malicious software dapat ditempuh dengan cara yang instan. Yaitu dengan menggunakan perangkat yang dikenal dengan nama virus generator. Nama lain dari perangkat jenis ini adalah virus kit, atau virus constructor, atau virus construction kit, atau virus creator, atau virus generation kit, dll. Dengan perangkat ini seseorang dengan kemampuan pemrograman yang minim atau bahkan seseorang yang tidak mengetahui bahasa pemrograman pun dapat membuat dan menghasilkan sebuah virus. Contoh virus generator diantaranya adalah

- Biological Warfare,
- Virus Creation Laboratory,
- Ultras Contruction Kit,

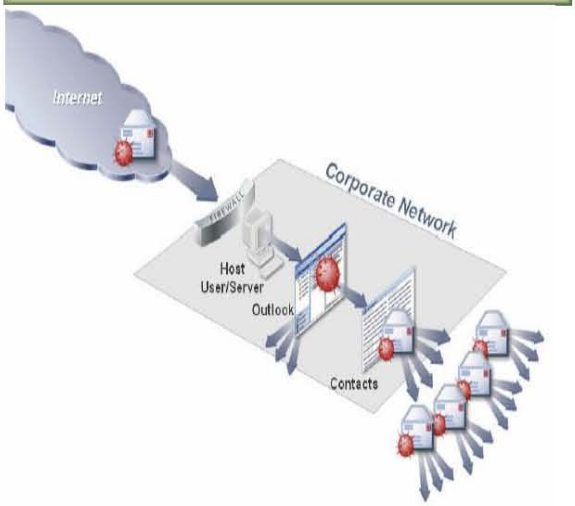
- Walrus Macro Virus Generator,
- Bio Hazard,
- Dav's Delphi Worm Generator,
- Indra VBS Worm Generator,
- Kagra VBS Worm Generator,
- Microsoft Macro Virus Generator,
- Microsoft Macro Virus Generator,
- Microsoft Visual Basic Script Worm Editor,
- TVBSG Visual Basic Script worm generator,
- Uber Worm Generator,
- VBS Worm Generator,
- Fast Firus Engine, dll.



Gambar I.1 Virus generator Fast Firus Engine buatan Fajar Anggiawan

Dari banyak jenis-jenis malicious software yang paling luas dikenal masyarakat adalah virus, worm, dan trojan horse. Virus berasal dari bahasa latin yang berartinya racun. Memperbanyak dirinya dengan cara menginfeksi file yang lain. Baik dengan metode appending, prepending, atau overwriting. Payload atau efek yang dibawa pun beragam dari yang tidak berbahaya sampai yang agresif dan sangat berbahaya seperti memformat harddisk. Semua payload tergantung dari programmernya.

Malicious software yang kedua adalah worm. Berbeda dari virus, worm tidak menggandakan diri dengan menginfeksi file yang lain. Worm menggandakan diri dengan membuat copy dari dirinya sendiri. Payload atau efek yang dibawa pun beragam tergantung dari pembuat atau programmer wormnya. Worm menyebar dengan menunggangi email. Worm ini menyisip ke badan email dalam bentuk *attachment* atau lampiran. Kemudian dengan memanfaatkan address book (buku alamat) yang ada pada aplikasi email client semacam Outlook, worm akan menggandakan diri dan menyebar ke Internet kembali.



Gambar I.2 Penyebaran worm melalui email

Malicious software yang ketiga adalah trojan horse. Berbeda dari virus dan worm, trojan horse tidak menggandakan diri. Dan untuk payload (efek) yang dibawa pun beragam tergantung dari pembuat atau programmer trojan horse tersebut. Maka dari itu trojan horse biasa digunakan oleh para programmer malicious software untuk misi-misi khusus. Dalam artian dibuat untuk satu kepentingan sesuai kondisi dari target yang akan diserangnya.

Istilah malicious code mempunyai makna yang sama dengan malicious software. Menurut Onno W. Purbo dan Tony Wiharjito dalam bukunya Keamanan Jaringan Internet, malicious code adalah suatu program yang bila dieksekusi akan menyebabkan sesuatu yang tidak diinginkan di dalam sistem. User biasanya tidak memperhatikan program ini hingga ditemukannya kerusakan. Malicious code ini dapat menyebabkan kerusakan atau kehilangan data yang serius, penolakan terhadap servis dan jenis-jenis insiden yang lan.

II. PEMBAHASAN

Tulisan ini menjelaskan tentang worm I Love You dengan trojan horse Barok yang dibuat oleh Onel de Guzman. Tentu saja dengan benang merah diantara ketiganya.

- **Onel de Guzman**

Sebelumnya ia adalah seorang yang biasa saja dalam dunia komputer ini, seperti juga dengan orang-orang lain yang intens dalam dunia ini. Tidak banyak yang mengenal. Namanya mencuat tatkala ia disebut-sebut sebagai pembuat worm yang merupakan kambing hitam terhadap kerugian besar di bumi ini. Onel de Guzman hanyalah seorang mahasiswa dari AMA Computer College di kota Makati, Filipina. Seandainya dia tidak tersangkut masalah ini, tentu dia dapat lulus dari College-nya secara terhormat.

Anak muda ini merupakan salah seorang anggota dari sebuah kelompok komputer yang bernama Grammersoft. Kelompok ini – seperti diungkap CNN – telah beberapa kali mencoba untuk meng-hack ISP terbesar di negeri itu yaitu Moscom Internet. Dan setidaknya dua kali menyebarkan virus secara sengaja ke para pelanggan Moscom. Penulis kira Onel de Guzman dengan Grammersoft berusaha untuk mencari jalan dalam rangka mendapatkan akses internet secara gratis. Perlu diketahui bahwa pada saat itu akses Internet di Filipina tergolong tinggi dan dihitung per jam. Satu jam akses dihargai sekitar 100 Peso atau setara dengan 2 sampai 3 US Dollar. Kalikan saja dengan 8.300 untuk mendapatkan besaran dalam Rupiah. Walhasil, untuk berlama-lama mengakses Internet di sana hanyalah milik orang-orang borjuis saja. Inilah yang kemudian bermuara pada dibuatnya I Love You dan juga trojan Barok yang dapat Anda simak selanjutnya di artikel ini.

Gambar II.1. Onel de Guzman

Sebuah Thesis yang Kandas

Seperti pada umumnya mahasiswa, mereka juga diharuskan membuat suatu proyek sebagai bagian dari tugas perkuliahan dan juga sebagai tugas akhir untuk kelulusannya. Tidak terkecuali Onel de Guzman. Sebagai seorang mahasiswa, anak muda ini, yang cerdas dalam pemrograman, juga mengajukan proposal thesis. Judul yang diajukan ke para dosennya adalah "**Email Password Sender Trojan**". Dari judulnya saja Anda bisa berkata bahwa ini adalah sebuah judul yang dapat membuat 'bulu kuduk seseorang berdiri'. Cukup seram untuk sebuah judul thesis. Dengan ruang lingkup yang dibahas adalah 'software product' alias pembuatan program.

Email Password Sender Trojan dalam thesis Onel de Guzman merupakan sebuah trojan sederhana yang dapat mengirimkan password-password seseorang ke email account yang telah

ditentukan. Password yang dikirimkan adalah password screen saver, web, RAS (Remote Access Server), dan termasuk cache password. Cache password adalah password yang tersimpan di Windows untuk kemudahan user sehingga ia tidak perlu mengetikkannya lagi. Ia hanya disamarkan dengan karakter tertentu, tetapi karakter aslinya tetap ada. Windows akan menyimpannya untuk kemudahan Anda bila opsi 'Save password' diaktifkan. Contoh fitur Windows yang memanfaatkan cache password adalah **Dial-Up Networking** bila Anda akan mengakses Internet. Windows menyediakan kemudahan untuk user dalam berinteraksi dengan komputer dan Windows juga yang menyediakan kemudahan sehingga cache password tersebut dapat dicuri.

Onel de Guzman dalam thesisnya berpendapat bahwa program yang dia buat akan bermanfaat bagi orang banyak untuk mendapatkan password Windows. Misalnya untuk mendapatkan Internet Account seseorang sehingga dapat ber-Internet ria tanpa perlu membayar. Bagaimana menurut Anda ide ini? Suatu kesenangan di atas penderitaan orang lain. Proposal yang diajukan Onel de Guzman kandas. Kampusnya menolak usulan proposal thesis tersebut dan menganggapnya melanggar etika.

- **I Love You**

Siapa yang tidak mengenal virus I Love You. Virus ini mencetak hit pada seputar bulan Mei tahun 2000. Boleh dibilang hampir semua pengguna komputer mengenal virus ini, setidaknya pernah mendengarnya, karena daya sebarnya yang luar biasa sehingga menggemparkan dunia. Kerugian yang diakibatkan virus ini ditaksir sekitar 7 Milyar dan bahkan mampu mencapai 10 Milyar US Dollar (CNN.com). Bisa jadi Anda pernah dikirimi I Love You.

I Love You yang mempunyai nama lain Lovebug atau Love Letter, sebenarnya merupakan sebuah worm. Memperbanyak diri dengan meng-*copy* dirinya dan mampu membawa rutin-rutin destruktif yang tidak diinginkan user. Tepatlah bila worm ini digolongkan ke dalam *malicious software*, alias program jahat.

Worm ini mulai ditemukan pada tanggal 4 Mei 2000 (F-Secure). Dalam kondisi ini worm dikatakan *in the wild*. Sudah berada di dunia luar, lepas dari laboratorium dan tersebar luas. Bila worm masih berada pada komputer pembuatnya, masih berada pada komputer Onel de Guzman dan belum tersebar ke luar, maka diistilahkan berada dalam keadaan *in the zoo*.

Setiap virus, worm, dll mempunyai suatu tanda yang membedakannya dengan 'organisme' yang lain. Pada badan worm I Love You juga terdapat signature atau tanda yang merupakan ciri khasnya seperti di bawah ini:

rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila, Philippines

Sedikit penulis jelaskan tentang signature I Love You tersebut. Spyder merupakan nama samaran buat Onel de Guzman di dunia cyber. (Bila yang dia maksudkan adalah laba-laba, harusnya dia menyebut Spider dan bukan Spyder). Rem merupakan singkatan dari kata *remark* yang artinya komentar. Dalam bahasa pemrograman BASIC, tulisan-tulisan (*statement* program) yang ada setelah rem dianggap sebagai komentar dan tidak akan dieksekusi oleh kompiler. Dalam pemrograman, rem bermanfaat

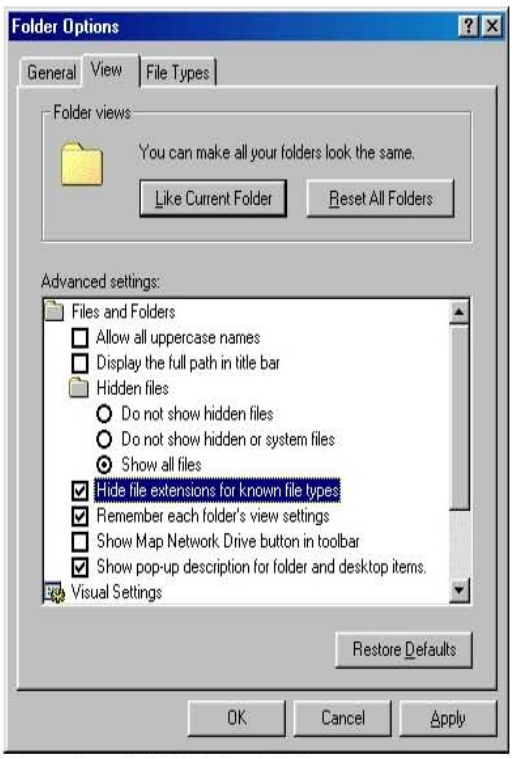
untuk mempermudah pelacakan kesalahan, memberi tanda, atau untuk memberi komentar suatu kode atau blok program, sehingga dapat mempermudah programmer lain membaca kode programnya. Silakan Anda buka buku tentang pemrograman BASIC. Sembarang tulisan dapat ditambahkan setelah rem. Di sini Onel de Guzman memanfaatkannya sebagai pengenal worm I Love You.

Gambar II.2. Virus I Love You datang dalam bentuk attachment suatu email

Efek Destruktif I Love You

I Love You menyebar melalui email sebagai surat berantai (*chain letter*). Daya sebar I Love You tergolong cukup cepat. Pada tanggal 8 Mei 2000 pukul 05:00 PM CERT Coordination Center menerima laporan lebih dari 650 situs individu yang mengindikasikan 500.000 sistem individu yang terinfeksi I Love You. Persebaran yang cepat dimungkinkan karena I Love You memanfaatkan buku alamat pada Outlook untuk melakukan *mass mailing*. I Love You akan mengirim email berisi *copy* dirinya ke setiap alamat yang ada pada buku alamat tersebut. Sehingga worm ini digolongkan ke dalam **@mm** (menyebar melalui email secara mass mailing). Berbeda dengan **@m** yang menyebar hanya lewat email yang Anda kirim keluar.

I Love You mengganti dan menambahkan beberapa tipe file. Diantaranya file-file dengan ekstensi *.jpg atau *.jpeg menjadi file dengan penambahan *.vbs. Semisal file **Gambar.jpg** akan menjadi **Gambar.jpg.vbs**. Selain itu dia juga melakukan hal yang sama pada file-file dengan ekstensi *.mp3 atau *.mp2. Untuk masalah ini yang perlu diperhatikan adalah bila Anda mengaktifkan fitur "**Hide file extension for known file types**" pada **Folder Options** Windows (lihat Gambar 3), maka penambahan ekstensi kedua (*.vbs) tidak akan nampak. Seolah-olah tidak ada perubahan sama sekali. Inilah yang dicoba untuk dimanfaatkan oleh worm I Love You.



Gambar II.3. Folder Options

Itu semua adalah sebagian contoh efek destruktif yang dibawa oleh worm I Love You. Tetapi efek destruktif tersebut akan tergolong kecil bila Anda melihat kemampuan berbahaya lain berikut ini yang dibawa oleh worm ini.

Efek yang berbahaya sekali adalah worm ini membuka gerbang untuk masuknya trojan yang telah disiapkan sendiri oleh Onel de Guzman. Worm I Love You akan memodifikasi Internet Explorer, tepatnya memodifikasi **Start Page IE**. Yang diubah adalah bagian registry Windows, yaitu pada key ini:

Hkey_Current_User\ Software\ Microsoft\ Internet Explorer\ Main\ Start Page

Key **Start Page** ini diarahkan pada salah satu dari empat alamat URL berikut ini yang ditentukan secara random (acak):

- "http://www.skyinet.net/~young1s/ ... /WIN-BUGSFIX.exe"
- "http://www.skyinet.net/~angelcat/ ... /WIN-BUGSFIX.exe"
- "http://www.skyinet.net/~koichi/ ... /WIN-BUGSFIX.exe"
- "http://www.skyinet.net/~chu/ ... /WIN-BUGSFIX.exe"

Keempat URL tersebut mengarah pada file yang sama yaitu WIN-BUGSFIX.exe. Akibatnya bila user menjalankan browser Internet Explorer maka akan langsung men-*download* file WIN-BUGSFIX.exe. Anda dapat mempraktekkan dengan mengubah registry Windows Anda dan kemudian menjalankan browser Internet Explorer, yang merupakan browser paling banyak digunakan orang di muka bumi ini.

Apa sesungguhnya file ini? Benarkah file ini merupakan *patch* untuk memperbaiki Sistem Operasi Windows yang memang banyak terdapat bug? Dan file ini hadir sebagai penolong? File ini pada hakekatnya adalah sebuah trojan yang membawa peran tersendiri. Onel de Guzman berharap ada orang yang tertipu dari manuver yang dibuatnya.

Tidak sampai di situ, ada juga bagian lain yang diubah untuk memuluskan skenario ini. Bagian registry Windows yang dimodifikasi lainnya adalah pada key ini:

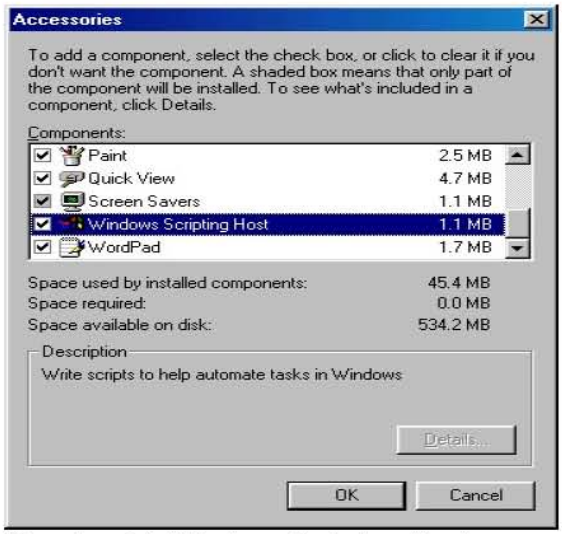
Hkey_Local_Machine\Software\Microsoft \Windows\CurrentVersion\Run\WIN-BUGSFIX

Key ini berfungsi untuk memaksa Windows untuk menjalankan file yang telah di-*download* tersebut setiap kali Windows dimulai.

Penulis kira inilah peran khusus dari worm I Love You. Setelah file WIN-BUGSFIX.exe berhasil di-*download* dan Windows siap menjalankan file ini, maka peran worm ini selesai. Peran selanjutnya dijalankan oleh file WIN-BUGSFIX.exe yang sejatinya merupakan trojan pencuri password.

Windows Scripting Host

I Love You dibuat dengan menggunakan bahasa Visual Basic Script, sehingga mempunyai ekstensi *.vbs. Sebagaimana dengan script-script Visual Basic lainnya, I Love You tidak dapat bekerja bila Anda menonaktifkan atau tidak meng-*install* Windows Scripting Host. Ini adalah satu cara melindungi diri dari serangan I Love You. Tetapi bila Anda memutuskan untuk menonaktifkan Windows Scripting Host, maka pertimbangkanlah script-script yang lainnya, karena bisa tidak berjalan juga.



Gambar II.4. Windows Scripting Host

Windows Scripting Host dapat Anda akses melalui fitur Add/Remove Programs Properties di Control Panel. Pada gambar 1 memperlihatkan komponen Windows Scripting Host yang telah ter-*install*. Perhatikan bagian Description pada kotak dialog tersebut. Pada bagian itu Microsoft sendiri menjelaskan bahwa Windows Scripting Host dapat digunakan untuk mengotomatisasikan tugas-tugas dalam Windows. Ini adalah satu sinyalemen. Otomatisasi adalah bagai pisau bermata dua. Dengan otomatisasi tugas-tugas Anda menjadi mudah dan cepat. Ini berarti satu keuntungan dalam proses produksi atau bekerja. Tetapi jangan lupa, dengan otomatisasi pula segalanya dapat berjalan dengan sendirinya padahal tidak diinginkan oleh user, berjalan diluar kontrol user yang menggunakan komputer itu. Ini satu sisi lain yang bersifat negatif. Dalam koridor otomatisasi, yang berperan penting adalah rutin-rutin yang dijalankan. Hal ini tergantung oleh sang programmer.

- **Barok**

Sebagaimana telah dijelaskan dimuka bahwa I Love You berperan membuka jalan bagi penyebaran dan penetrasi trojan yang telah disiapkan oleh Onel de Guzman ke komputer sasaran. Selanjutnya peran diambil alih oleh trojan.

Barok disebar oleh I Love You dari 4 alamat URL pada webserver Skylnet. Trojan Barok ini seperti trojan-trojan lainnya mempunyai dua bagian. Yaitu bagian client dan server. Tetapi berbeda dengan kebanyakan trojan yang ada, trojan Barok bukanlah dari tipe *remote controlling* yang mendominasi sebagian besar trojan di muka bumi ini. Barok berbeda dari Back Orifice atau SubSeven yang telah penulis bahas juga di bagian lain dari buku ini. Untuk lebih jelasnya mari kita lihat dua bagian dari trojan Barok ini.

Trojan Barok yang banyak beredar di Internet ada beragam versi dari Barok 1.0, Barok 2.0, dan Barok 2.1. Pada penulis terdapat Barok versi 2.0 dengan ukuran paket zip sebesar 335 KB. Ada tiga file pada paket tersebut, tetapi intinya hanya dua bagian yaitu file **Client.exe** dan **Server.exe**.

Gambar II.5. About Barok 2.0

Gambar II.6. Client Barok 2.0

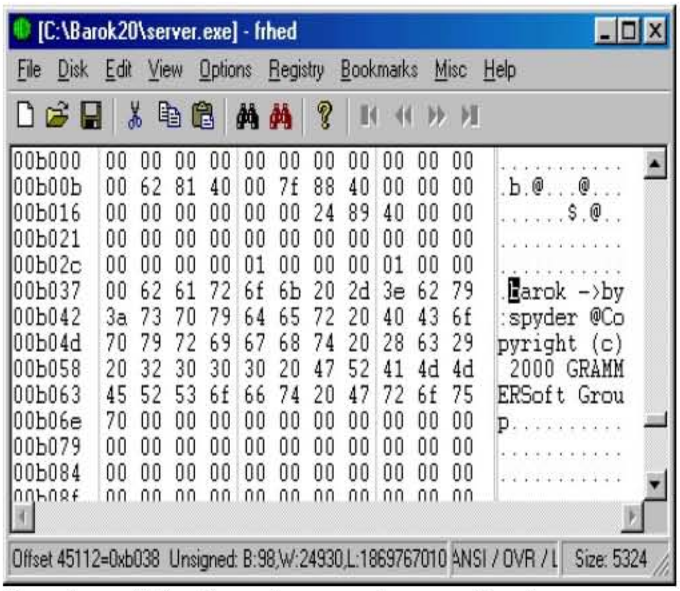
Trojan Barok merupakan trojan yang dapat dikonfigurasi. Bagian **Client** merupakan unit untuk mengkonfigurasi bagian **Server**. Bagian yang dapat dikonfigurasi pada **Client Barok** adalah :

- File name
- Outgoing Mail Server (SMTP)
- Destination Mail
- Schedule Send.

Barok dibuat oleh Spyder dan GrammerSoft (Lihat gambar About Barok 2.0). Untuk memprogram Client dan Server Barok ini Onel de Guzman menggunakan Microsoft Visual C++. Hal ini dapat diketahui dengan 'pembedahan' Barok menggunakan hexeditor. Diantaranya pada offset A59C file Server.exe dan pada offset D6A8C file Client.exe terdapat informasi yang menunjukkan tentang hal ini.

Signature atau tanda juga terdapat pada Barok sebagai pengenal bahwa file tersebut adalah trojan Barok. Pada bagian server, yaitu mulai di offset B038 terdapat signature ini:

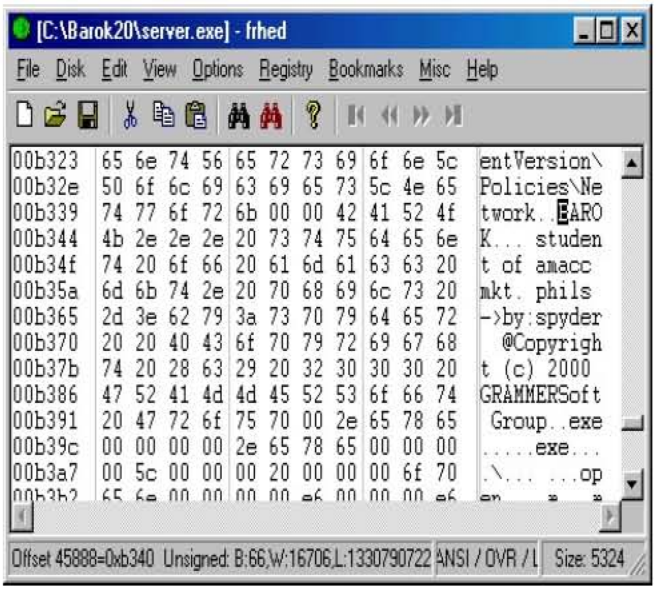
barok ->by:spyder @Copyright (c) 2000 GRAMMERSoft Group



Gambar II.7. Signature pertama Barok Server

Signature lainnya dapat dilihat pada offset B340, akan Anda jumpai seperti di bawah ini:

BAROK...student of amacc mkt. phils ->by:spyder @Copyright (c) 2000 GRAMMERSoft Group



Gambar II.8. Signature kedua Barok Server

Berdasarkan pengujian yang penulis lakukan terhadap trojan Barok ini, baik unit Client ataupun unit Server, telah terdeteksi oleh Antivirus McAfee.

III. KESIMPULAN

Antara Onel de Guzman, I Love You dan Barok merupakan suatu mata rantai yang saling berkait. Anak muda yang berusia 24 tahun itu – usia yang sama ketika Chen Ing Hau membuat virus CIH – membagi peran untuk I Love You dan Barok dalam rangka mencuri password Windows untuk kepentingan pribadi. Satu hal yang tidak diperkenankan dalam aturan manapun. Bagi kita semua tentu harus bersikap kritis dan meningkatkan kewaspadaan walaupun terhadap virus, worm atau trojan yang terlihat sepele sekalipun. Karena bisa jadi dia merupakan satu mata rantai dari skenario besar yang sedang berjalan. Mencegah lebih baik dari mengobati.

DAFTAR PUSTAKA

Anoname. June 2008. Malicious Software (Malware): A Security Threat to The Internet Economy. OECD Ministerial Meeting on The Future of the Internet Economy.

Chandraleka, Happy. 2004. Virus, Worm, dan Trojan Horse. Penerbit Andi. Yogyakarta.

Chandraleka, Happy, 2004. Keylogger dan Pemrogramannya. Penerbit Andi. Yogyakarta.

Ferbrache, David dan Mort, Stuart. 1997. Malicious Software and Hacking. CRC Press, Inc. Florida.

Purbo, Onno W., dan Wiharjito, Tony. 2000. Keamanan Jaringan Internet. Penerbit Elex Media Komputindo. Jakarta.

Tucker, Allen B. 1997. The Computer Science & Engineering Handbook. CRC Press, Inc. Florida.

Wai, Anthony. 2008. Malicious Software Threats and Protection.

http://www.hkcert.org/ppt/event119/2.malware_mcafee.pdf.