ISSN: 1978 - 8282

TEKNIK MEMBONGKAR PERTAHANAN VIRUS LOKAL MENGGUNAKAN VISUAL BASIC SCRIPT DAN TEXT EDITOR UNTUK PENCEGAHAN

Junaidi [1]
Sugeng Santoso [2]
Sugeng Widada [3]

junaidiskom@yahoo.com, ciwi212@yahoo.com

ABSTRAKSI

Pesatnya perkembangan virus lokal belakangan ini yang terkadang menginfeksi komputer, menuntut harus mulai berfikir mengambil bagian tentang bagaimana cara pembuatan pencegahnya. Hal ini diperlukan, karena virus lokal terkadang sulit dideteksi oleh beberapa antivirus terkemuka, kecuali oleh beberapa antivirus buatan lokal yang kemudian dipublikasikan sebagai antivirus yang mampu menangani satu atau beberapa jenis virus lokal. Hal ini bisa terjadi mungkin saja disebabkan karena virus lokal bekerja tidak sebagaimana virus non lokal pada umumnya, sehingga keluar dari standar pencarian virus, contohnya saja jarang sekali virus lokal yang menginfeksi file exe atau file com atau yang lainnya, sehingga sangat sulit dideteksi sebagai virus atau bukan, kecuali ketika virus tersebut telah dilaporkan dan terdeteksi oleh pembuat antivirus, baru virus tersebut dapat diatasi, lagi-lagi tercipta asumsi bahwa virus selangkah lebih maju dari antivirus. Salah satu penyebab dari sulitnya mendeteksi virus lokal ini, karena hampir tidak ada bedanya dengan file biasa, apalagi virus ini juga menggunakan bahasa lokal. Satu sisi mungkin bisa berbangga, karena beberapa nama virus lokal merupakan bahasa Indonesia, dan telah menjadi nama yang berada di database daftar virus internasional. Kini saatnya mencoba membongkar pertahanan virus lokal secara manual, yang mungkin suatu saat teknik ini akan mampu menciptakan antivirus secara sederhana. Teknik membongkar pertahanan virus lokal menggunakan bahsa visual basic script dan teks edior mengacu pada target pengamanan beberapa bagian vital yang diinfeksi oleh virus, seperti registry, msconfig, sysedit, cmd, folder windows, system32 dan masih banyak lagi. Hal ini dimaksudkan bahwa dengan memahami teknik membongkar pertahahanan virus tentunya diharapkan mampu mencegah virus menginfeksi komputer lebih dini, hal ini sejalan dengan asumsi bahwa mencegah lebih baik dari mengobati.

Kata Kunci : Virus, Registry, Infeksi, Perlindungan, Pencegahan

1. **Dosen Jurusan Teknik Informatika, STMIK Raharja**
   Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692
2. **Dosen Jurusan Teknik Informatika, STMIK Raharja**
   Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692
3. **Dosen Jurusan Teknik Informatika, STMIK Raharja**
   Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692

PENDAHULUAN

Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya. Virus dibuat untuk mengubah, memanipulasi bahkan sampai merusak. Virus hanya akan bekerja apabila program pemicu atau program yang telah terinfeksi dieksekusi.

Sebagai perumpamaan, agar lebih memahami tentang teknik membongkar pertahanan virus lokal menggunakan bahasa visual basic script dan teks editor, terlebih dahulu posisikan sebagai dokter. Seorang dokter dalam memahami penyakit pasiennya, harus tahu bagaimana penyakit tersebut menular, dengan apa dan cara apa virus menular, akan merusak jaringan syaraf yang mana, atau akan berakibat buruk pada anggota tubuh yang mana, dan masih banyak lagi kemungkinannya, dengan demikian, dokter dapat membuat atau memberikan obatnya.

Begitu juga dengan virus, kalau ingin mencegah dan melindungi komputer dari virus, terlebih dahulu harus mengenali virus yang akan dicegah, atau dari virus apa saja komputer dilindungi. Tentunya akan bertanya, kenapa tidak pakai antivirus saja, bukankan lebih praktis dan lebih aman. Pembahasan ini bukan bermaksud mengabaikan antivirus yang telah ada, tetapi bagaimana mencoba untuk menghentikan aktivitas virus dikomputer tanpa menggunakan antivirus, tentunya virus lokal yang dibuat dengan visual basic dan hampir rata-rata membutuhkan keterlibatan *registry*. Dan juga sama-sama pernah merasakan bahwa suatu saat sebuah antivirus tidak dapat mengatasi virus yang baru, sementara disisi lain ada antivirus yang telah mampu. Hal ini sangat tergantung dari perkembangan dan kemampuan antivirus itu sendiri. Kejadian ini sangat dimungkinkan terjadi, karena virus selangkah lebih maju dari antivirus.

Secara garis besar antivirus dapat diartikan sebagai program yang dapat menangkap, mengidentifikasi dan menghancurkan virus. Dalam ruang lingkup pemanfaatannya terdapat tiga kelompok antivirus, antara lain :

1. *Fix* yang merupakan sebuah program yang dapat mendeteksi dan menghancurkan hanya satu virus, harus dijalankan terlebih dahulu kemudian program akan mencari dan menghapus virus tertentu.
2. Antidot yang merupakan sebuah program yang dapat menangkap, mendeteksi beberapa jenis virus dan menghapusnya, sama seperti program *fix*, harus dijalankan terlebih dahulu kemudian akan mencari file yang terinfeksi maupun file virus tertentu.
3. Antivirus yang merupakan sebuah program yang dapat menangkap, mendeteksi dan menghapus banyak jenis virus. Dapat otomatis menangkap file yang terinfeksi dan menghapusnya.

Untuk dapat memahami lebih jauh tentang pencegahan dan perlindungan dari virus lokal menggunakan visual basic, ada baiknya memahami dulu tentang apa itu virus, bagaimana teknik penyerangannya dan apa saja yang dapat dilakukan virus serta bagian apa saja yang akan diserang virus.

Berbekal dari pengalaman yang berkali-kali terserang virus, hingga berkali-kali pula melakukan pemformatan dan penggantian hardisk, pada akhirnya mulai tertarik untuk meneliti dan mempelajari bagaimana virus dibuat, tentunya sesuai dengan kemampuan dalam pemrograman visual basic, penulis mulai melakukan berbagai percobaan dan pengkajian. Diawali dengan melepaskan antivirus, membiarkan virus masuk untuk kemudian menangkapnya dan membongkarnya, hingga pada akhirnya memahami bagaimana teknik penyerangan dan pertahanan virus. Semua ini dilakukan karena jika ingin melumpuhkan virus, maka harus terlebih dahulu memahami sistem dan strategi virus dalam melakukan aktivitasnya.

Diawali dengan terbongkarnya beberapa virus lokal yang dibuat dengan *visual basic script*, penulis melakukan beberapa penyesuaian dengan visual basic dan windows API, untuk mengakses *registry* yang telah terinfeksi virus, hal ini diperlukan karena virus hasil penggandaan yang disimpan pada beberapa folder sistem dan windows disembunyikan, kemudian fasilitas untuk menampilkan file yang tersembunyi pada folder option di windows explorer pun diblokir, hingga pemblokiran berlangsung di *regedit, msconfig, sysedit, cmd* dan lain sebagainya. Disinilah awal ketertarikan untuk mulai mempelajari virus dalam hal teknik penyerangan sistem, penggandaan diri dan pertahanan dari ancaman, hingga sampai pada persembunyian, perkenalan, gangguan dan pengrusakan. Dan pada akhirnya dipaparkan secara terbuka pada artikel yang berjudul "**Teknik Membongkar Pertahanan Virus Lokal Menggunakan Visual Basic Script dan Text Editor Untuk Pencegahan".**

Dari paparan diatas tentunya akan muncul pertanyaan, bagaimana mungkin virus dapat dicegah sedemikian rupa tanpa menggunakan antivirus?. Bagian apa saja yang harus diperbaiki agar virus dapat dihapus?. Bagaimana cara membuka beberapa fasilitas yang sebenarnya dapat menghentikan virus, sementara fasilitas tersebut diblokir?, bisakah visual basic melakukan semua itu untuk mencegah dan melindungi sistem komputer?.

Walaupun akan membahas tentang t**eknik membongkar pertahanan virus lokal menggunakanVisual Basic Script dan Text Editor untuk pencegahan**, penulis

membatasi pembahasan hanya pada teknik pencegahan dan perlindungannya dengan menggunakan perintah visual basic, tidak sampai pada tahap pembuatan antivirus sebenarnya, yang mampu melacak keberadaan virus dan menghentikan virus ketika ingin menyerang sistem, hal ini lebih difokuskan pada teknik membongkar beberapa fasilitas yang diblokir dan kemudian melakukan pemusnahan virus melalui fasilitas tersebut yang berhasil diselamatkan.

PEMBAHASAN

Untuk dapat membuat program sederhana dalam pencegahan dan perlindungan dari virus lokal, ada beberapa hal yang harus dikuasai secara standar, dalam hal ini cukup menguasai pemrograman visual basic standar, minimal bisa membaca alur program. Kemudian memahami sistem operasi windows, minimal mengerti menjalankan windows explorer, mencari keberadaan file, mengerti cara mengatur tampilan file pada windows explorer, apakah menampilkan semua file atau menampilkan file yang tidak di hidden saja, mengerti cara merubah attribut file, mengerti cara mengcopy dan menghapus file. Kemampuan berikutnya adalah mengerti tentang *registry windows*, cara membuka *registry*, membaca *registry*, menambahkan *key, string* dan *value* pada *registry*, dan mengetahui daerah serangan virus. Untuk lebih jelasnya tentang beberapa kemampuan tersebut, berikut akan dibahas satu persatu secara bertahap.

1. Daerah Rawan Yang Menjadi Target Serangan Virus.
   Ini adalah standar virus lokal tentang daerah apa saja yang akan diserang oleh virus, memang ada beberapa yang tidak standar, namun biasanya file inti dari sebuah virus tidak jauh berada di folder windows, system32 dan lain sebagainya. Kalau pun tidak berada disana, bisa melacaknya melalui *registry* windows, tentunya fasilitas *registry* harus tidak terblokir. Yang jelas, virus pasti berusaha masuk ke sistem yang ada di komputer untuk mengunci sistem, memanipulasi dan mengganti sistem tersebut agar virus dapat lebih leluasa berkembang biak.

2. *Registry* Windows Sebagai Target Utama Serangan Virus Lokal
   Registry windows merupakan suatu database untuk menyimpan dan mengatur sistem di windows. *Registry* windows merupakan otak dari sistem operasi windows yang dijalankan, *registry* windows akan selalu dibackup oleh sistem dalam hitungan waktu tertentu, *registry* windows juga akan melakukan backup pada saat melakukan shutdown. Dengan *registry* windows, dapat melakukan beberapa perubahan dan perbaikan terhadap sistem, bahkan dapat melakukan beberapa pengaturan untuk meningkatkan kinerja windows, memanggil beberapa file pada saat startup dan lain sebagainya. Karena keberadaan *registry* windows yang sangat

vital ini, maka *registry* menjadi sasaran utama virus untuk melakukan beberapa pengaturan yang terkait dengan persiapan-persiapan aktivitas virus. Berikut adalah *registry* windows yang dijalankan melalui klik start à run à ketik regedit. (Lihat Gambar-1)

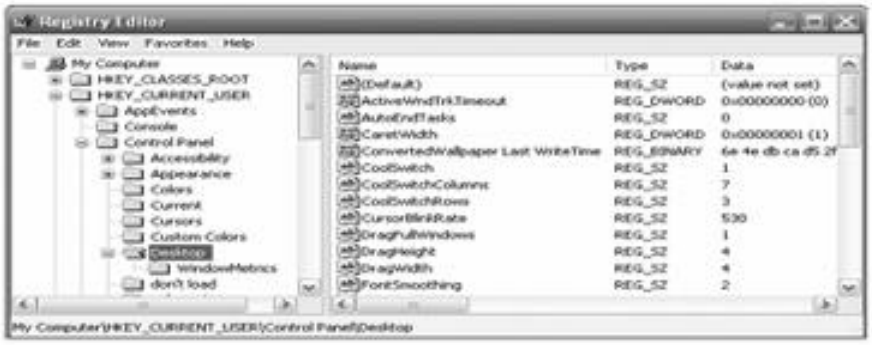
Gambar 1
Registry Windows

2.a. Kunci Utama *Registry* Windows

Registry windows terdiri dari 5 Key sebagai kunci utama yaitu HKEY_CLASSES_ROOT (HKCR), HKEY_CURRENT_USER (HKCU), HKEY_LOCAL_MACHINE (HKLM), HKEY _USERS (HKU) dan HKEY_CURRENT_CONFIG (HKCC). HKCC mempunyai *Key Software* dan *Key System*. Dan *Key System* mempunyai anak lagi yaitu *Current Control Set*, dan *Key Current Control Set* mempunyai anak *Key Control* dan *Key Enum*, dan seterusnya yang tidak dapat dijelaskan secara rinci disini.
(Lihat Gambar-1)

2.b. Setiap Kunci Utama (*Key*) Pada *Registry* Memiliki Nilai (*Value*)

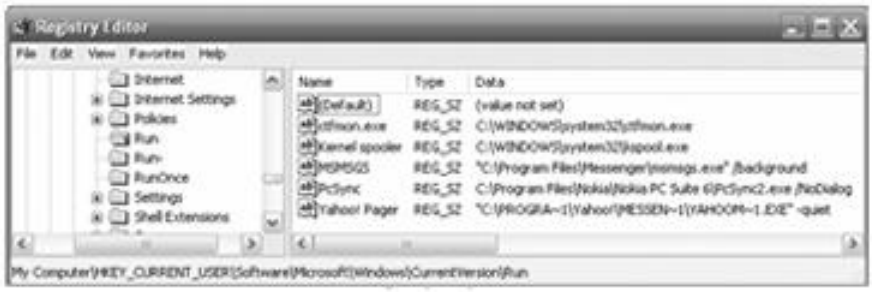
Value merupakan isi dari setiap key yang ada di *registry* windows. Dilihat dari tipe datanya, value memiliki 3 jenis data, yaitu DWORD dengan jenis angka atau inte ger, STRING dengan jenis karakter (huruf) atau kalimat, BINARY dengan jenis angka biner, dan masih ada beberapa jenis lain, namun tidak dibahas karena jarang dipakai dalam *registry* itu sendiri. (Lihat Gambar-2)



Gambar 2
Registry Windows

2.c. Alamat *Registry*

Dalam hal pengaturannya, *registry* windows mempunyai alamat yang berguna untuk mengatur konfigurasi pada windows, misalnya :
Untuk menjalankan suatu aplikasi secara otomatis, dapat dilihat pada alamat (Lihat Gambar-3)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\

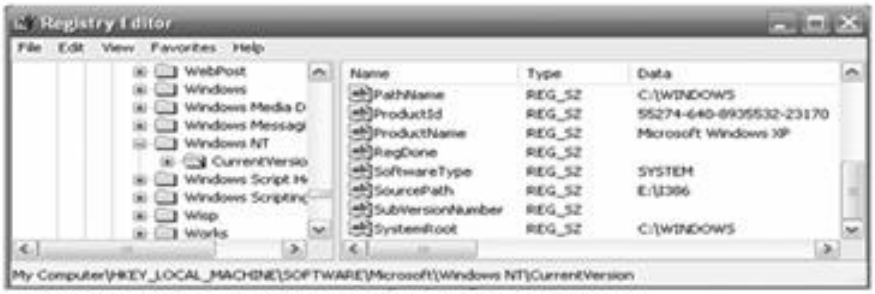


Gambar 3
Registry Windows

Untuk memanipulasi kode explorer, dapat dilihat pada alamat (Lihat Gambar-4) :
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\

Gambar 4
Registry Windows

Untuk memanipulasi drive penginstalan, lisensi pada windows, dapat dilihat pada alamat (Lihat Gambar-5) :
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\



Gambar 5
Registry Windows

Perlu diingat bahwa beberapa alamat di *registry* sangat riskan untuk di rubah, terkadang hal tersebut menjadi "senjata makan tuan" jika tidak berhati – hati dalam pengubahan *registry* tersebut, karena akan berakibat sistem menjadi *crash*.

3. *Registry* Sasaran Virus Lokal

Dari sekian banyak alamat *registry* yang memiliki fungsi masing-masing, hanya sebagian alamat *registry* saja yang menjadi sasaran virus untuk mengatur penyerangan dan perlindungan virus yang biasa di exploitasi oleh virus lokal. Paling tidak jika menemukan virus lokal, sebaiknya cek di alamat *registry* ini:

3.a. *Registry* Mengaktifkan Virus Lokal

Berguna untuk memicu file virus agar otomatis aktif pada saat startup, virus akan mengakses alamat ini dan memberikan nilai alamat dimana file virus berada, dan akan selalu aktif setiap kali startup, dengan alamat (Lihat Gambar-3):

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

2.b. *Registry* Menyembunyikan *Extension* File

Pada alamat *registry* ini biasanya digunakan untuk menyembunyikan extension file. Biasanya virus menyembunyikan extension file untuk menipu user, seperti yang dilakukan oleh sebagian virus lokal, hal ini dapat dilakukan pada *registry* dengan alamat (Lihat Gambar-4) :

Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer \Advanced\
Key : HideFileExt
Value : 1

2.c. *Registry* Menyembunyikan File *Hidden*

Alamat *registry* ini berguna untuk menyembunyikan file dengan atribut hidden. Jadi untuk mempertahankan kelangsungan hidupnya, virus menyembunyikan diri dengan mengatur file beratribut hidden. Walaupun sebenarnya ada teknik lain, yaitu dengan membuat nama file utama virus mirip dengan nama system file di windows, misalnya file *svchost, lsass, csrss*, dan lain – lain, nama file tersebut mirip dengan nama file system yang ada pada windows, alamat *registry* untuk menyembunyikan file yang beratribut hidden tersebut adalah (Lihat Gambar-4) :

Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer \Advanced\
Key : Hidden
Value : 0

File yang beratribut hidden pada windows explorer ditandai dengan icon yang kabur. file tersebut dapat disembunyikan dengan alamat *registry* di atas tadi.
Sehingga pada windows explorer, semua file yang beratribut *hidden* tidak akan terlihat, begitu juga dengan file virus dalam menyembunyikan dirinya. file virus

tidak akan terlihat karena file tersebut diatur dengan atribut hidden.

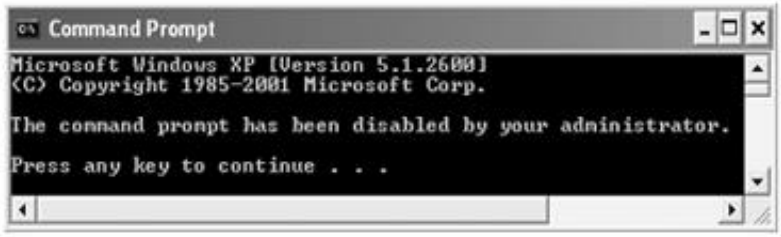
2.d. *Registry* Memblokir Regedit

Gambar 6 :
Pesan *registry* yang diblokir

Registry ini berguna untuk mengunci regedit yang ada di windows. Sehingga bila mencoba masuk ke *registry*, maka akan muncul pesan pemblokiran (Lihat Gambar-6).

Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\
Key : Disable*Registry*Tools
Value : 1

2.e. *Registry* Memblokir Command Prompt



Gambar 7
Pesan command prompt yang diblokir

Registry ini berguna untuk mengunci command prompt. Sehingga bila mencoba masuk ke command prompt, maka akan timbul pesan pemblokiran (Lihat Gambar 7).

Alamat : HKCU\Software\Policies\Microsoft\Windows\System\
Key : DisableCMD
Value : 1

2.f. *Registry* **Memblokir** *Task Manager*

Gambar 8
Pesan task manager yang diblokir

Registry ini berguna untuk mengunci *Task Manager*. Sehingga bila mencoba masuk ke *Task Manager*, maka akan timbul pesan pemblokiran (Lihat Gambar-8).

Alamat : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\
Key : DisableTaskMgr
Value : 1

2.g. *Registry* Memblokir System Restore

Registry ini berguna untuk mengunci *system restore*. Sehingga bila mencoba masuk ke *system restore*, maka akan timbul pesan pemblokiran (Lihat Gambar-9).

Gambar 9
Pesan system restore yang diblokir

Alamat : HKLM\Software\Policies\Microsoft\Windows NT\SystemRestore\
Key : DisableSR
Value : 1

3. System Editor (SysEdit)

Gambar 10
Tampilan Layar System Editor

Selain virus menyerang daerah *registry*, virus juga akan menyerang sysedit atau sistem editor. System editor atau yang biasa disingkat dengan *Sysedit* adalah file tertentu yang dijalankan. ketika komputer masuk ke windows pertama kali, seperti halnya *regedit*. *Sysedit* ini biasanya masih banyak dipakai di sistem operasi windows lama seperti win95, Win98, Win3.1, walaupun memang sudah lama, secara tidak langsung berpengaruh juga pada user yang memakai sistem operasi windows XP. Untuk melihat *sysedit* ini klik StartàRunàKetik sysedit (Gambar 10).

Jadi sebenarnya dalam sysedit ini, bisa memanipulasi file yang pertama kali dieksekusi oleh windows ketika windows berjalan di komputer anda. File yang dimaksud dapat dijelaskan sebagai berikut :

3.a. Config.sys

Config.sys adalah file yang memuat tentang seluruh konfigurasi windows dan dijalankan ketika pertama kali windows mulai. Letak file ada di drive C:\ dan mempunyai atribut file system dan hidden.

3.b. Autoexec.bat

Autoexec.bat adalah file yang berisi perintah yang ada di komputer dan akan dijalankan pertama kali ketika windows berjalan. Letak file ada di drive C:\ dan mempunyai atribut file system dan hidden.

3.c. Win.ini

Win.ini juga sebuah file yang dieksekusi pertama kali oleh windows. File ini berisi tentang aplikasi 16 bit yang di-support oleh windows.

3.d. System.ini

System.ini adalah sebuah file yang berguna untuk menyimpan data font yang diakses oleh windows ketika pertama kali.

4. System Configuration Utility (MsConfig)

Dari aplikasi MsConfig, seluruh file system editor (*sysedit)* tadi dijalankan. Dapat dijalankan dengan melakukan klik *StartRun*àketik msconfig kemudian enter, maka akan muncul aplikasi seperti berikut (Lihat Gambar 11) :

Gambar 11
Tampilan Layar MsConfig

klik salah satu bar yang ada di aplikasi MsConfig tersebut. Misalnya klik baràS*ervices* maka akan muncul gambar seperti di bawah ini :

Gambar 12
Tampilan Layar MsConfig à Services

Dari gambar 12 di atas jelas terlihat daftar file (services) yang dijalankan oleh services ketika windows berjalan pertama kali. Tapi para virus biasanya menggunakan *MSCONFIG* ini untuk menjalankan program virus mereka secara otomatis, yaitu dengan memanipulasi bar startup.

Gambar 13
Tampilan Layar MsConfig à Startup

Dari gambar 13 di atas jelas terlihat daftar file yang dijalankan pada saat melakukan startup, misalnya saya daftar file pada baris pertama, terlihat jelas bahwa item VPTray dijalankan dengan perintah memanggil file yang ada di bagian *command*.

5. Folder Yang Sering Menjadi Target Serangan Virus Untuk Pertahanan
   Selain akan menginfeksi *registry*, virus juga akan menggandakan diri ke beberapa folder yang dianggap penting dan rawan, hal ini dimaksudkan agar keberadaan virus tetap eksis dan sulit diketahui oleh pemakai, karena pada umumnya file yang

berada pada folder-folder penting dianggap rawan untuk dihapus, sebab akan mempengaruhi kinerja sistem. Adapun alamat folder yang sering adalah : c:\windows, c:\windows\system, c:\windows\system32

IMPLEMENTASI

Cara Kerja Pencegahan Dan Perlindungan Dari Virus Lokal

Cara kerja teknik pencegahan dan perlindungan dari virus lokal ini adalah kebalikan dari virus itu sendiri, terutama dalam hal infeksi *registry*. Hal ini dimaksudkan agar dapat mengakses *registry*, *command prompt, msconfig* dan masih banyak lagi, sehingga dapat melacak keberadaan file induk virus lokal yang dimaksud, mengetahui bagaimana virus tersebut menyerang, bertahan, dan pada bagian apa saja virus tersebut melakukan berbagai perubahan.

KESIMPULAN

Dari seluruh paparan diatas, dan setelah membahas tentang rekayasa teknik pencegahan dan perlindungan dari virus lokal menggunakan visual basic dan API dapat disimpulkan bahwa terdapat beberapa folder yang menjadi sasaran virus untuk menggandakan dirinya dalam rangka untuk menyerang dan bertahan. Dan juga dapat disimpulkan bahwa *registry* merupakan syarat mutlak untuk diinfeksi oleh virus lokal, karena sebagian besar virus lokal yang dibuat dengan bahasa pemrograman visual basic yang berjalan di microsoft windows melakukan pengaturan di *registry*.

Infeksi ini dilakukan, dalam rangka melakukan beberapa pengaturan agar virus dapat bekerja sesuai apa yang direncanakan, serta melakukan beberapa pemblokiran fasilitas penting untuk melindungi dirinya. Teknik pencegahan dan perlindungan ini dapat dilakukan dengan berusaha membuka beberapa fasilitas yang diblokir, hal ini dapat dikatakan sebagai bentuk kebalikan dari apa yang dilakukan oleh virus dalam mengatur registry.

DAFTAR PUSTAKA

1. Junaidi (2006). Memburu Virus RontokBro Dan Variannya Dalam Membasmi Dan Mencegah. Cyber Raharja, 5(3), 82-99.

2. Rahmat Putra (2006). *Innovative Source Code Visual Basic*, Jakarta: Dian Rakyat.

3. Slebold, Dianne (2001). *Visual Basic Developer Guide to SQL Server.* Jakarta: Elex Media Komputindo.

4. Stallings, William (1999). *Cryptography and Network Security*. Second Edition. New Jersey: Prentice-Hall.Inc

5. Tri Amperiyanto (2002). Bermain-main dengan Virus *Macro*. Jakarta: Elex Media Komputindo.

6. Tri Amperiyanto (2004). Bermain-main dengan *Registry* Windows. Jakarta: Elex Media Komputindo.

7. Wardana (2007). Membuat 5 Program Dahsyat di Visual Basic 2005. Jakarta : Elex Media Komputindo.

8. Wiryanto Dewobroto (2003). Aplikasi Sains dan Teknik dengan Visual Basic 6.0. Jakarta: Elex Media Komputindo.

ISSN: 1978 - 8282

PEDOMAN PENULISAN

Lingkup Jurnal. Tulisan yang dapat dimuat adalah yang mengkaji masalah yang berhubungan dengan bidang ilmu komputer dan teknologi informasi, baik ilmudasar maupun aplikasinya.

Jenis tulisan. Tulisan dapat berupa laporan/hasil penelitian atau makalah ilmiah bukan penelitian seperti laporan studi kasus atau kajian pustaka komprehensif. Tulisan ilmiah/penelitian dapat merupakan hasil a) Pengembangan, b) Penemuan, dan c) Pembuktian

A. Laporan penelitian minimal harus memuat bagian abstrak, pendahuluan (latar belakang, t ujuan, hipotesis, konsep2 utama), metodologi, hasil dan pembahasan, kesimpulan dan pustaka.

B. Makalah ilmiah bukan penelitian minimal harus memuat bagian abstrak, pendahuluan, pembahasan, kesimpulan dan pustaka.

Nama Penulis. Ditulis tanpa gelar dan jabatan, disebutkan nama Lembaga dan alamatnya serta alamat e-mail.

Bahasa. Ditulis dalam bahasa Indonesia atau bahasa Inggris dengan memperhatikan kaidah-kaidah bahasa ragam ilmiah. Khusus untuk yang menggunakan bahasa Indonesia, hindari penggunaan kata ganti orang.

Panjang Tulisan. Panjang tulisan 10-15 halaman A4 spasi single termasuk tabel dan gambar serta lampiran, dengan jenis huruf Times New Roman, font 11.

Abstrak. Panjang abstrak maksimum 250 kata, dalam satu paragraf, dilengkapi dengan kata-kata kunci pada bagian akhir abstrak. Abstrak memuat latarbelakang, metodologi, hasil dan kesimpulan. Abstrak tidak bersifat matematis, tidak berisi saran dan harapan, tidak ada kutipan. Kata kunci (*keywords*) adalah kata-kata penting yang digunakan untuk mengidentifikasikan isi dokumen, dapat berupa metode/alat yang dipakai, variabel yang diteliti atau substansi penelitian. Abstrak ditulis dalam bahasa Indonesia dan Inggris.

Tabel dan gambar. Tabel dan gambar harus diberi nomer dan judul lengkap serta harus diacu dalam tulisan. Gambar dan tabel dalam format hitam putih.

Persamaan. Persamaan matematik harus diberi nomer urut dalam kurung biasa ,(x), dengan penulisan rata kanan.

Setiap makalah diwajibkan untuk mengutip sumber pustaka yang berasal dari jurnal ilmiah nasional maupun internasional.

Kutipan. Setiap kutipan harus menyertakan sumbernya yang ditulis pada

kutipan, yaitu dengan menuliskan nama belakang pengarang pertama (jika pengarang lebih dari satu: dituliskan nama pengarang pertama et al), dan tahun terbit. Contoh : .....menurut Angel (2003), atau .....(Angel, 2003), atau ..... Chen et al(2007)

Pustaka. Pustaka disusun terurut berdasarkan nama belakang pengarang dan hanya memuat pustaka yang dikutip dalam tulisan. Nama pengarang ditulis tanpa gelar, jika ada nama tengah dan belakang, disingkat. Contoh :

Buku.

1. Angel (2003). *Interactive Computer Graphics: A Top-Down Approach Using OpenGL*. Third Edition. London: Pearson Education.
2. Irianto (2004). *Embedding Pesan Rahasia Dalam Gambar*. Bandung: Institut Teknologi Bandung.

Tulisan/artikel dalam buku.

1. Bolton, MA: Anker Publisher Inc, 144-158. Yudhana, A (2007). Desain Routing Trafik Jaringan Telekomunikasi dengan algoritma Genetik, dalam Wibowo, T.A (Ed), *Berbagai Makalah Sisitem Informasi,*
2. Olanivan, B.A (2004). Computer-mediated Communication as an instruction learning tool: course evaluation with communication students, in Comeaux, P(Eds), *Assessing Online Teching&Learning*,
3. *Prosiding Konferensi Nasional Sistem Informasi 2007*, Bandung : Departemen Teknik Informatika, Sekolah Tinggi Teknologi Telkom, 233-238.

Jurnal.

1. Goyal, D.P (2007). Information Systems Planning Practices in Indian Public Enterprises. *Information Management & Computer Security,* 15(3), 201-213

Sumber online.

1. Chen, CC., Wu, J., Yang, SC. (2007). *The Efficacy of online cooperative l earning systems. The perspective of task-technology fit*. Diakses pada 20 Mei 2007 dari : http: // www emeraldinsight.com/1065-0741.htm.
2. Marques, O., Baillargeon, P (2007). *Design of multimedia traffic classifier for snort*. Diakses pada 2 Juni 2007 dari : http: // www.emeraldinsight com/0968-5527.htm.

Redaktur Pelaksana

Maimunah, S. Kom.

FORMULIR PERSETUJUAN PEMBUATAN ARTIKEL JURNAL	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-003
PENANGGUNG JAWAB	**MENYETUJUI**
KETUA STMIK RAHARJA	
DIREKTUR AMIK RAHARJA INFORMATIKA	
TENTANG/PERIHAL/JUDUL	
Judul terlampir :	
Abstraksi terlampir :	
BAGIAN PENULIS	**MEMOHON**
Nama Penulis Naskah/Pengarang 1	
Nama Penulis Naskah/Pengarang 2	
Nama Penulis Naskah/Pengarang 3	
Nama Editor/Penyunting	
Nama Penyunting/Picture Layout & Artistik	
KETUA EDITOR	**MEREKOMENDASIKAN**
Reviewer 1	
Reviewer 2	

ISSN: 1978 - 8282

FORMULIR **KRITERIA DAN BOBOT PENILAIAN** **KARYA TULIS ILMIAH**	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-001

Kode Judul : _____

Judul Karya Tulis Ilmiah : _____

_____

_____

Reviewer : ☐ Mitra Bestari ☐ Dewan Redaksi

Nama Reviewer : _____

NO	KRITERIA (NILAI MAKSIMAL)	INDIKATOR PENILAIAN	HASIL PENILAIAN NARATIF DAN SARAN	NILAI SETIAP KRITERIA
1.	**JUDUL (5)**	A. Maksimal 14 (empat belas) kata dalam Bahasa Indonesia atau 10 (sepuluh) kata dalam Bahasa Inggris **(1)** B. Relevan dengan isi sangat jelas **(2)** C. Relevansinya dengan permasalahan sangat jelas **(2)**		
2.	**ABSTRAK (5)**	A. Dalam Bahasa Indonesia dan Bahasa Inggris yang baik **(5)** jika hanya dalam Bahasa Indonesia yang baik atau Bahasa Inggris yang baik **(2.5)** B. Format sesuai dengan pedoman **(1)** C. Isi : Latar belakang metode, hasil, dan kesimpulan tertuang dengan kalimat yang jelas **(4)**		

3.	**SISTEMATIKA (15)**	A. Sesuai dengan Pedoman **(5)** B. Ada Instrumen pendukung (gambar, grafik) dan sangat relevan **(5)** C. Daftar pustaka : dominan terbitan 10 (sepuluh) tahun terakhir dan pustaka primer **(5)**		
4.	**SUBSTANSI (70**	A. Data/informasi telah diolah dengan sangat baik **(10)** B. Relevansi latar belakang dan pembahasan sangat jelas **(15)** C. Analisis dan sintesis atau pembahasan sangat baik **(25)** D. Kesimpulan : sangat jelas relevansinya dengan latar belakang dan pembahasan, dirumuskan dengan singkat **(20)**		
TOTAL NILAI MAKSIMAL				

Hasil Penilaian:*

☐ Diterima ☐ Diterima dengan baik ☐ Ditolak

……, ……

Mitra Bestari / Dewan Redaksi

Keterangan:

**** Hasil penilaian: nilai total > 75, makalah diterima***

Catatan untuk redaksi pelaksana:

1. Tulisan yang dikirim kepada pemeriksa, nama penulisnya ditutup, dan diganti nomer kode.
2. Setiap tulisan diperiksa oleh dua orang, satu orang dari dewan redaksi dan satu orang dari mitra bestari.

ISSN: 1978 - 8282

FORMULIR **EDITOR BAHASA KARYA TULIS ILMIAH**	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-004

Kode Judul : _____

Judul Karya Tulis Ilmiah : _____

_____

_____

Editor : ☐ Editor Bahasa

Nama Editor : _____

Saya yang bertanda tangan di bawah ini menyatakan semua tulisan/kalimat sesuai dengan kaedah EYD, atau sesuai dengan kaedah-kaedah tata bahasa.

Catatan:

Rekomendasi: *

☐ Diterima ☐ Diterima dengan perbaikan ☐ Ditolak

Tangerang, _____

_____

Editor

Keterangan:

**** Rekomendasi diisi berdasarkan hasil pemeriksaan editor***

ISSN: 1978 - 8282

FORMULIR **EDITOR LAYOUT DAN ARTISTIK** **KARYA TULIS ILMIAH**	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-005

Kode Judul : _____

Judul Karya Tulis Ilmiah : _____

_____

_____

Editor : ☐ Editor Layout dan Artistik

Nama Editor : _____

Saya yang bertanda tangan di bawah ini menyatakan bahwa desain untuk layout dan artistik sudah format jurnal CCIT yang ditentukan.

Catatan:

Rekomendasi: *

☐ Diterima ☐ Diterima dengan perbaikan ☐ Ditolak

Tangerang, _____

_____

Editor

Keterangan:

**** Rekomendasi diisi berdasarkan hasil pemeriksaan editor***

FORMULIR PENYELESAIAN ARTIKEL	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-006
TENTANG/PERIHAL/JUDUL ARTIKEL:	

BAGIAN	KETERANGAN
Nama Penulis Naskah/Pengarang 1	☐ Lengkap
Nama Penulis Naskah/Pengarang 2	☐ Lengkap
Nama Penulis Naskah/Pengarang 3	☐ Lengkap
Nama Editor/Penyunting	☐ Lengkap
NamaPenyunting Picture/Layout & Artistik	☐ Lengkap
Nama Peninjau (Reviewer) 1	☐ Lengkap
Nama Peninjau (Reviewer) 2	☐ Lengkap
Nama Percetakan	☐ Lengkap

MENYETUJUI

KETUA DEWAN EDITOR

(.....)

SEKRETARIS REDAKSI

(.....)

ISSN: 1978 - 8282

FORMULIR **KESEDIAAN MITRA BESTARI** **JURNAL ILMIAH**	Tanggal Revisi : 12 Desember 2007 Tanggal Berlaku : 13 Desember 2007 Kode Dokumen : FM-RHJ-016-002

Yang bertanda tangan di bawah ini :

Nama Lengkap : _____

Jenjang Pendidikan : _____

Bidang Keahlian : _____

Jabatan Fungsional : _____

Pengalaman ReviewerJurnal : Ya / Tidak *), jika Ya sebutkan dimana, kapan nama jurnal yang di review:

_____

Bersedia menjadi reviewer ahli / Mitra Bestari Jurnal Ilmiah yang berada di bawah naungan Perguruan Tinggi Raharja.

Demikian formulir ini saya tanda tangani untuk dapat dipergnakan sebagai mana mestinya.

Tangerang, _____

Mengetahui, Mitra Bestari,

(.....) (.....)

*) Coret yang tidak perlu