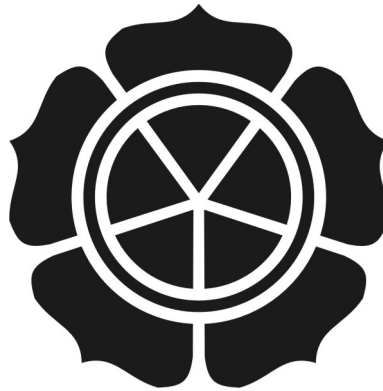


**APLIKASI PERTAHANAN TERHADAP SERANGAN MALCODE  
(MALICIOUS CODE) DALAM SISTEM OPERASI MICROSOFT  
WINDOWS XP PROFESIONAL SERVICE PACK 2**

**Naskah Publikasi**



diajukan oleh

**Nugroho Jati**

**06.12.2025**

kepada

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM  
YOGYAKARTA**

**2010**

# NASKAH PUBLIKASI

## Aplikasi Pertahanan Terhadap Serangan Malcode (Malicious Code) Dalam Sistem Operasi Microsoft Windows XP Profesional Service Pack 2

disusun oleh

**Nugroho Jati**

**06.12.2025**

**Dosen Pembimbing**




**Melwin Syafrizal, S.Kom, M.Eng**

**NIK. 190302105**

**Tanggal, 21 Juli 2010**

**Ketua Jurusan**

**Sistem Informasi**



**Drs. Bambang Sudaryatno, MM**

**NIK. 190302029**

***DEFENDER APPLICATION FROM ATTACKED BY MALCOE  
(MALICIOUS CODE) ON OPERATING SYSTEM MICROSOFT  
WINDOWS XP PROFESIONAL SERVICE PACK 2***

***APLIKASI PERTAHANAN TERHADAP SERANGAN MALCODE  
(MALICIOUS CODE) DALAM SISTEM OPERASI MICROSOFT  
WINDOWS XP PROFESIONAL SERVICE PACK 2***

Nugroho Jati  
Jurusan Sistem Informasi  
STMIK AMIKOM YOGYAKARTA

***ABSTRACT***

*The need for information recently made a lot of organizations providing public services to its customers better; whether it is information services, trade, culinary, electronics, application (software) and others, where most of the information displayed in the virtual world (Internet) and can not be denied that there was goodness there where there is also a crime.*

*An expert in the field of programming (programmers) are a misuse of science for society disturbed or interfere with the application of artificial spread of a destructive nature, or better known as the malcode, malware, malscript or perhaps better known by the people called computer viruses, whereby when the application is implemented, then the condition of the operating system owned by a customer will be disrupted and even destroyed.*

*This paper, trying to provide solutions to people who had been in contact with other people in a positive interaction of course and through cyberspace (the Internet), where the computer has been infected application or malcode better known destroyer of ordinary people as computer viruses, so malcode is eradicated from the computer and fix the registry files as well as the damaged structure, using an application called antidote or with antivirus.*

***Keywords:*** *Malcode (Malicious Code), antivirus, application, people*

## 1. Pendahuluan

Perkembangan zaman saat ini senantiasa mempengaruhi pola pikir manusia untuk selalu berperan aktif mengikuti adanya perkembangan tersebut agar mampu bertahan dan mengembangkan pola kehidupannya. Termasuk teknologi yang erat dengan kehidupan manusia yang biasa disebut dengan komputer. Sama halnya manusia yang pernah sakit, komputer rumahan atau dikenal dengan sebutan PC(*Personal Computer*) pun dapat terserang penyakit yang mengganggu kinerja keseluruhan PC(*Personal Computer*) tersebut yaitu dengan terinfeksi kode-kode pemrograman jahat atau yang biasa disebut malcode(*Malicious Code*) yang sering berkeliaran tak terkendali dan sengaja di buat oleh programmer yang tak bertanggung jawab.

## 2. LandasanTeori

### 2.1 Kualitas Informasi

Informasi dapat dikatakan berkualitas jika minimal memenuhi tiga hal, yaitu akurat(*accurate*), tepat waktu(*timeliness*) dan relevan (*relevance*).

Akurat(*accurate*), berarti informasi bebas dari kesalahan-kesalahan serta tidak bias yang dapat menyesatkan pengguna informasi tersebut. Keakuratan akan informasi juga harus jelas dan mencerminkan maksudnya.

Tepat waktu(*timeliness*), berarti bahwa informasi yang sampai ke pengguna tidak boleh terlambat, hal ini akan berpengaruh pada pengambilan keputusan.

Relevan (*Relevance*), berarti informasi mempunyai manfaat untuk pemakainya, dengan kata lain informasi tersebut diterima oleh orang yang memang membutuhkan informasi tersebut.

## 3. Analisis

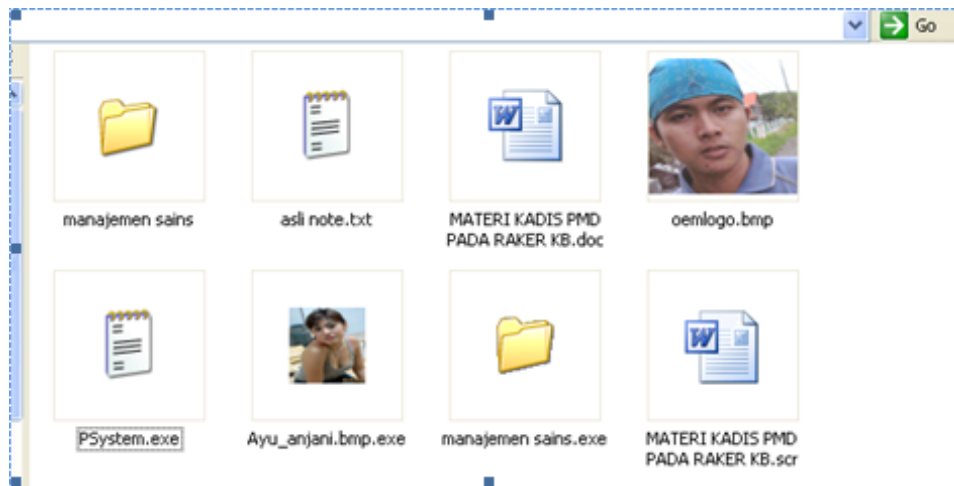
### 3.1 Fisik Malcode (Malicious Code Physical)

#### 3.1.1 Ikon Malcode (Malicious Code Icon)

Malcode melakukan serangan terhadap sasaran calon korbannya hampir selalu sama menggunakan teknik *Social Engineering*<sup>1</sup> atau cara mengelabui calon korbannya dengan ikon-ikon yang menyerupai ikon asli sistem seperti yang disebutkan dalam bab sebelumnya yaitu ikon folder, ikon notepad, ikon word standart, ikon picture standart dan termasuk juga menggunakan gambar-gambar yang syur atau panas.

---

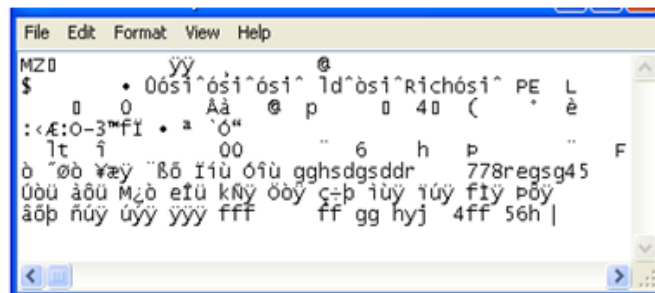
1 <http://ilmukomputer.org/2008/11/mengenal-social-engineering/> , *knowledge, e-learning*. diakses November 2009



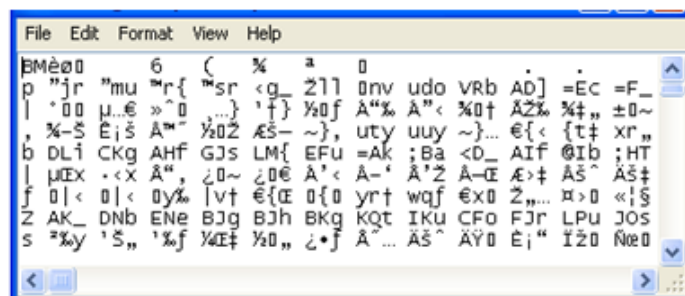
**Gambar 1** Perbandingan File Asli dengan File Terinfeksi

### 3.1.2 Header Malcode

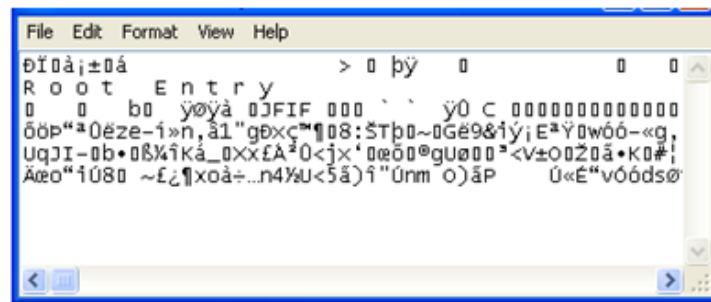
Pendeskripsian malcode selain ditinjau dari ekstensinya dapat juga diidentifikasi melalui headernya atau biasa disebut dengan induk pembacaan suatu data atau file agar dapat dimengerti dan diolah oleh mesin (*computer*) sehingga dimengerti oleh manusia (*user*). Lebih jelasnya nampak dalam gambar berikut



**Gambar 2** Header File bertipe Executable

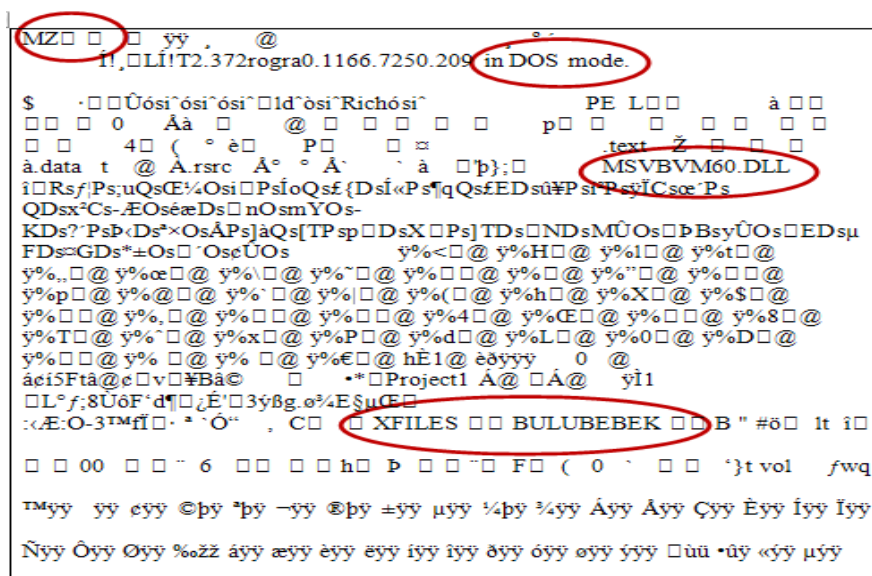


**Gambar 3** Header File bertipe Bitmap



**Gambar 4** Header File bertipe Document (Word)

Bila diperhatikan nampak pada awal string setiap file terdapat tulisan seperti "MZ, BM, Dİ" inilah yang disebut dengan header, dari setiap data atau file yang terdapat dalam sistem operasi windows pada umumnya, header file ini dianalisa dengan menggunakan notepad standar.



**Gambar 5** Header Worm BULUBE BEK dibuka dengan Notepad

Nampak awal string "header" file tersebut adalah "MZ" yang merupakan file eksekusi (executable) dan terdapat pula keterangan "in DOS mode" jelas ini merupakan malcode berjenis worm yang selalu bersarang di memory, jadi setiap sistem operasi dalam kondisi mulai (*start up*) worm ini berjalan, nampak pula keterangan "MSVBVM60.DLL" ini dijelaskan bahwa program ini di buat dengan Visual Basic versi 6.0, dan terlihat juga keterangan "XFILE BULUBE BEK" ini merupakan keterangan nama aplikasi tersebut yang merupakan malcode berjenis worm.

Pendeklarasian bilangan karakter kode Malcode memiliki kriteria bahasa sebagai berikut:

1. Bahasa Hexa : Bahasa yang dipahami dan di eksekusi oleh mesin atau komputer.
2. Bahasa Decimal : Bahasa yang dapat di pahami oleh manusia atau penggunanya (*brainware, user*)

**Tabel 1** Daftar Header File

Nama File	Ekstensi	Header
Executable	*EXE	MZ
Document	*DOC	DI
Bitmap	*BMP	BM
Image JPG	*JPG	JFIF
Image GIF	*GIF	GIF
Archiver File ZIP	*ZIP	PK
Archiver File RAR	*RAR	Rar!
Archiver File RAX	*RAX	rax!

Bahasa Hexa memiliki ciri yaitu dua karakter saling berdekatan yang mewakili satu karakter pada bahasa Decimal, berikut adalah beberapa bagian pemetaan antara bahasa Hexa dengan bahasa Decimal

**Tabel 2** Pemetaan Hexa dengan Decimal

BAHASA HEXA	BAHASA DECIMAL
00	. (titik)
3E	> (lebih besar)
A1	; (titik koma)
2A	* (bintang)
FF	Y (huruf "Y")
5A	Z (huruf "Z")
40	@ (at)

Karakter Malcode menggunakan cara penggabungan kedua bahasa tersebut diatas agar dapat melakukan pemblokiran program atau pembatasan hak akses pengguna(*user*), hasil penggabungan kedua bahasa disebut dengan Karakter HexaDecimal atau Harga HexaDecimal.

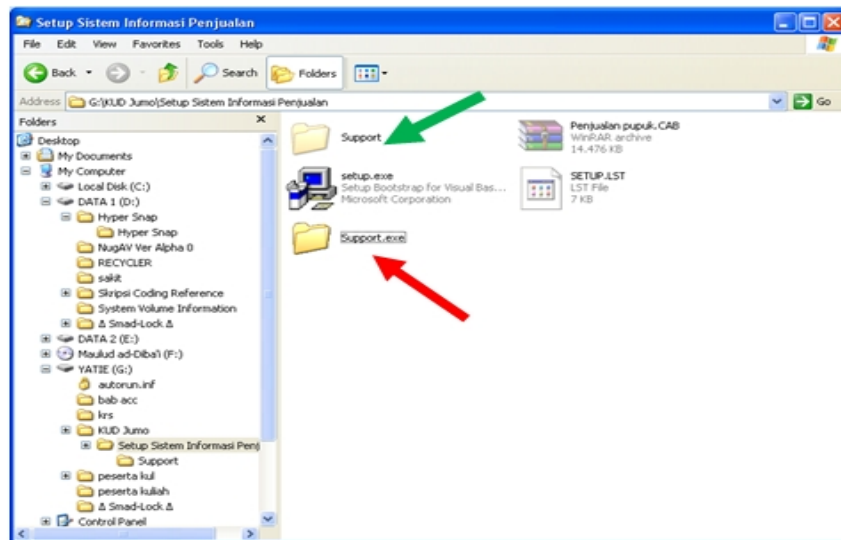
**Tabel 3** Pemetaan HexaDecimal dari Header File

Nama File	Ekstensi	Header	HexaDecimal
Executable	*EXE	MZ	4D 5A
Document	*DOC	DI	D0 CF
Bitmap	*BMP	BM	42 4D
Image JPG	*JPG	JFIF	4A 46 49 46
Image GIF	*GIF	GIF	47 49 46
Archiver File ZIP	*ZIP	PK	50 4B
Archiver File RAR	*RAR	Rar!	52 61 72 21
Archiver File RAX	*RAX	rax!	72 61 78 21



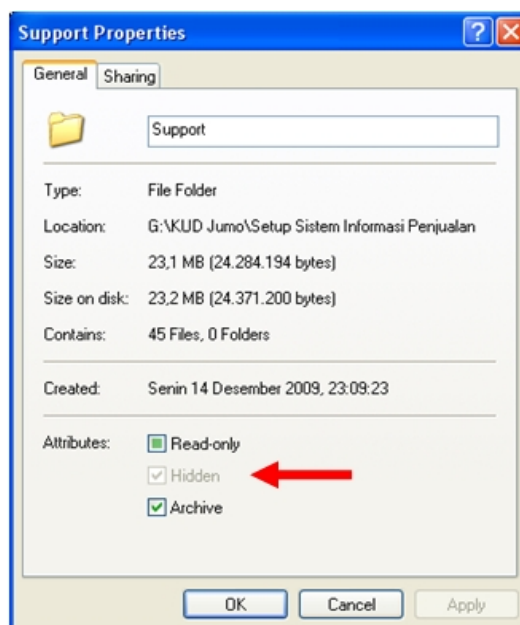
### 3.1.3 Serangan Malcode (System has been attacked by Malcode)

Serangan suatu malcode di dalam sistem seperti yang diterangkan sebelumnya yaitu salah satunya menyembunyikan file aslinya dan mengganti dengan file bayangan atau palsu, mengubah setiap file yang telah terinfeksi menjadi inang baru dalam penyebaran dan merusak sistem yang baru, membuat pertahanan dalam sistem operasi sehingga saat komputer dinyalakan (*start up*) akan ikut menghidupkan file-file malcode sehingga sulit untuk di musnahkan.



**Gambar 6** Serangan Malcode dalam Sistem

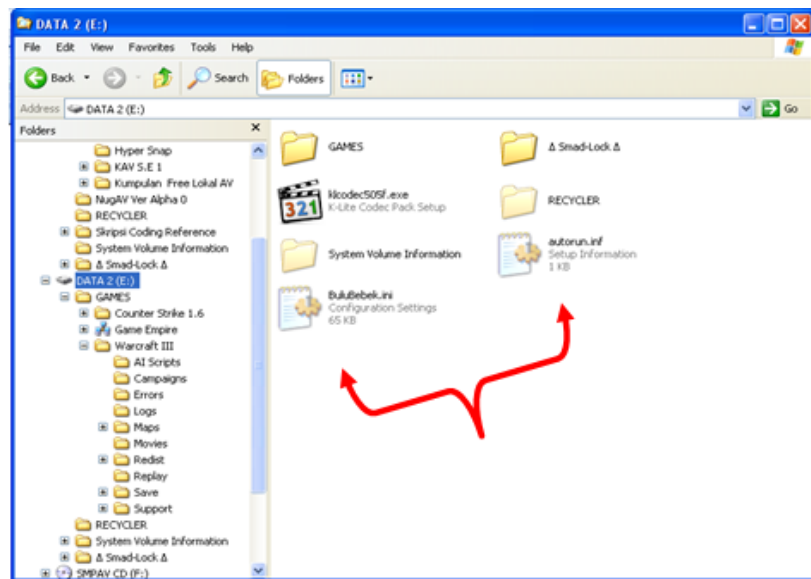
Nampak dalam gambar bahwa malcode telah melakukan serangannya ke dalam sistem sehingga seluruh file dan folder yang berada di dalamnya terinfeksi, gambar yang di tunjuk oleh anak panah berwarna hijau adalah file aslinya yang di buat menjadi tersembunyi (*hidden*) oleh malcode, dan gambar yang ditunjuk anak panah merah itu adalah file malcode atau file bayangan atau file penipu untuk memicu malcode makin merusak sistem.



**Gambar 7** Properties File atau Folder yang Dirusak oleh Malcode



Nampak dalam gambar anak panah berwarna merah menerangkan bahwa malcode telah membuat folder asli sistem menjadi tersembunyi (*hidden*) dan mengganti dengan file pemicu malcode dalam merusak sistem.



**Gambar 8** Pertahanan Malcode di dalam Sistem

Gambar anak panah berwarna merah menerangkan bahwa malcode telah membuat pertahanan dirinya di dalam sistem sehingga saat sistem operasi berjalan malcode tersebut ikut menjalankan dirinya pula sehingga menginfeksi seluruh file yang sedang beraktifitas di dalamnya, atau lebih mudahnya saat komputer di hidupkan malcode yang telah menginfeksi sistem operasi di dalam komputer tersebut ikut hidup pula.

Registry yang tersusun dalam sistem operasi ikut teracak-acak oleh aplikasi malcode yang telah menginfeksi sistem tersebut, sehingga setiap data di dalamnya ikut rusak atau sakit, inilah mengapa registry disebut juga sebagai jantungnya sistem operasi windows.

Hasil pelacakan dan analisa yang saya lakukan saat malcode tersebut aktif dan mengaktifkan ke-14 malcode jenis lain yang saya simpan, terhadap Autorun malcode yang menginfeksi sistem terdapat source code sebagai berikut.

[AUTORUN]

OPEN=BuluBebek.ini

shell\open=Open

shell\open\Command=BuluBebek.ini

shell\open\Default=1

shell\explore=Explorer

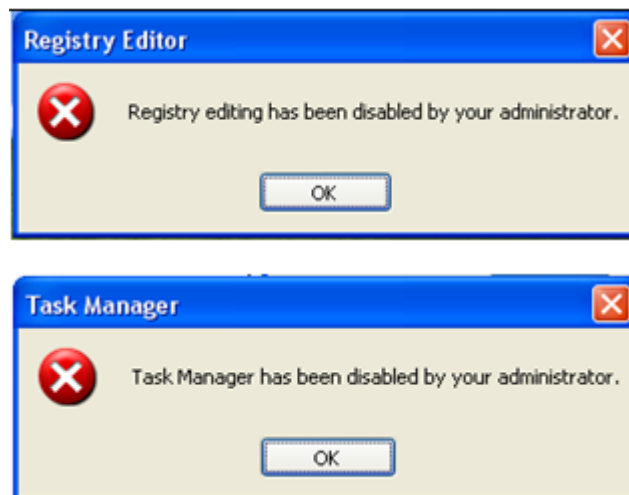
shell\explore\Command=BuluBebek.ini

Source code diatas menerangkan bahwa saat sistem dijalankan maka secara otomatis akan memanggil dan mengaktifkan malcode yang bernama “BuluBebek” dan menyembunyikan file asli keseluruhan yang berada di dalam “windows explorer” dan mengganti dengan file bayangan yang merupakan pemicu untuk menjalankan malcode BuluBebek.

Malcode jenis ini menerangkan bahwa jenisnya adalah worm dikarenakan ia bermukim di dalam memory komputer sehingga saat booting mulai-pun worm tersebut telah teraktifkan sehingga dapat membuat kapasitas memory bertambah dan menyebabkan kelebihan muatan (*overflow*).

#### 3.1.4 Memblokir Akses Fungsi Windows (Disable Functions of Windows)

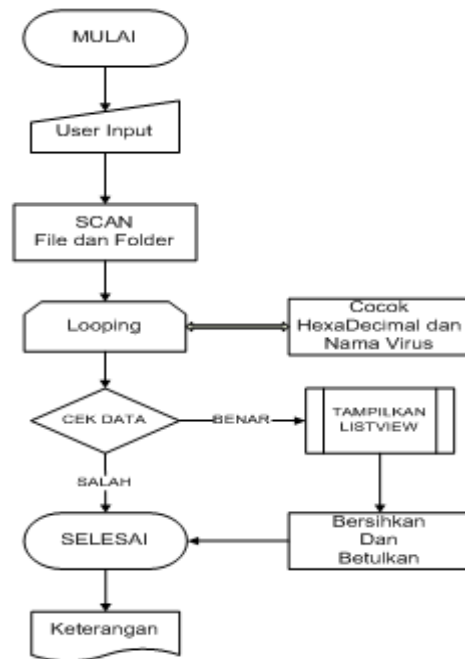
Hampir dapat dipastikan semua malcode akan memblokir fungsi windows dikarenakan fungsi tersebut dapat mengancam kelangsungan kehidupan malcode tersebut. Rangkaian fungsi yang dimatikan oleh malcode adalah *Task Manager*, *Registry Editor*, *ms Config*, *Folder Options*, *Run*, *Sistem Restore*, malcode melakukan pemblokiran tersebut setelah merubah, mengacak susunan registry dikarenakan 85% konfigurasi sistem operasi windows terdapat di dalamnya.



**Gambar 9** Registry Editor dan Task Manager yang Diblokir Aksesnya

#### 3.2 Alur Data Antivirus (Flowchart Antivirus)

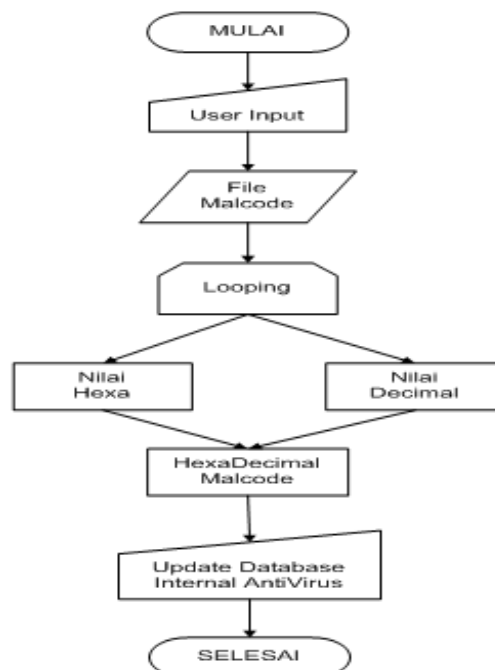
*Flowchart* atau dapat juga disebut dengan alur lalu lintas data dalam antivirus “NugAV ver Alpha 0” dimana termasuk di dalam Aplikasi Pertahanan Terhadap Serangan Malcode dalam Sistem Operasi Microsoft Windows XP Professional SP 2, dapat dilihat pada gambar di bawah ini:



**Gambar 10** Flowchart Antivirus NugAV ver Alpha 0

### 3.3 Flowchart Ceksum HexaDecimal

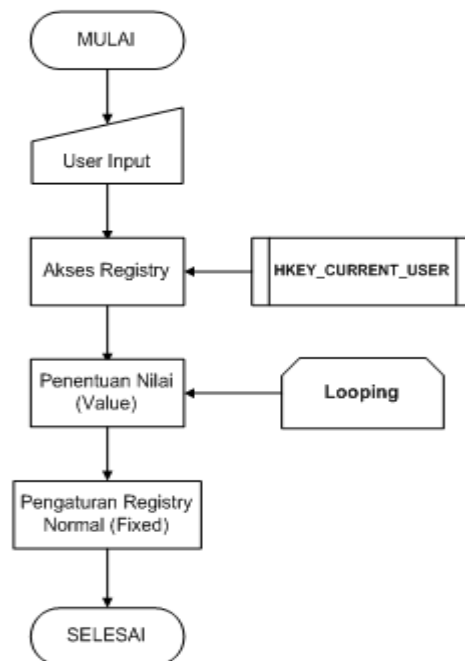
Menu ceksum turut membantu memberi dukungan umum dalam kinerja antivirus untuk lebih akurat dan tepat sasaran dalam mendefinisikan nama malware, ditelisik dan di jabarkan melalui nilai Hexa dan nilai Decimal dari setiap file yang diduga malware, kemudian disatukan dengan bentuk harga HexaDecimal malware.



**Gambar 11** Flowchart Ceksum HexaDecimal NugAV ver Alpha 0

### 3.4 Flowchart Penormal Registry (Registry Fixer)

Menu registry fixer ini juga turut berperan besar dalam menunjang kehandalan “NugAV ver Alpha 0” dimana setiap malcode pasti merubah struktur dan pengaturan registry, oleh karena itu menu ini di buat untuk kembali menormalkan struktur dan pengaturan registry dalam sistem operasi windows.



**Gambar 12** Flowchart Registry Fixer NugAV ver Alpha 0

### 3.5 Flowchart Malcode Keseluruhan (Virus, Worm, Trojan)

Alur data dipaparkan disini menjelaskan tentang pergerakan atau mobilitas yang dilakukan malcode dalam mengacak registry, merusak file, hingga merusak hardware. Melalui beberapa fase yaitu:

#### 1. Dormant Phase (Fase Tidur atau Istirahat)

Fase dimana malcode akan diaktifkan pada kondisi tertentu misalnya: tanggal atau waktu yang ditentukan, kehadiran atau dieksekusinya program lain, dan tidak semua malcode mencanangkan fase ini.

#### 2. Propagation Phase (Fase Perkembangbiakan)

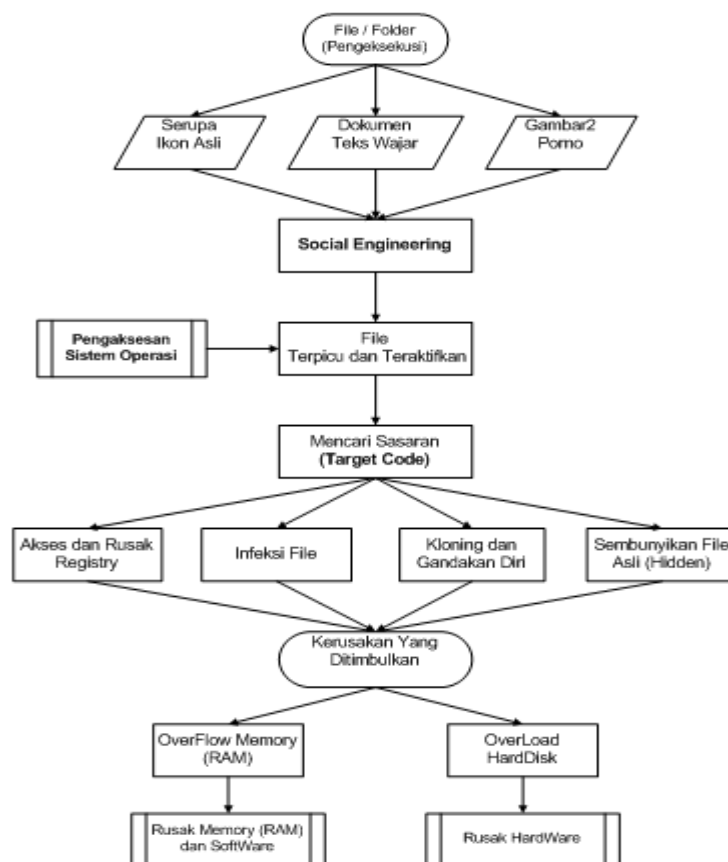
Fase ini disebut juga fase pengandaan diri yang ditujukan kepada program atau file atau media penyimpanan (*storage*) dan setiap file yang ternoda akan menjadi hasil kloning malcode atau akan bersifat malcode.

### 3. Triggering Phase (Fase Pemicu atau Pengaktifan)

Malcode menjadi hidup atau aktif dan mulai mencari sasarannya untuk menjalankan perintah yang ditanam dalam tubuh malcode, hal ini juga dipicu oleh kondisi di dalam *Dormant Phase*.

### 4. Execution Phase (Fase Eksekusi)

Fase dimana pelaksanaan eksekusi dasar yang ditanam di dalam tubuh malcode direalisasikan seperti menghapus file, menyembunyikan file asli, reboot atau restart serta menampilkan perintah lain.



**Gambar 13** Flowchart Malcode Keseluruhan (Virus, Worm, Trojan)

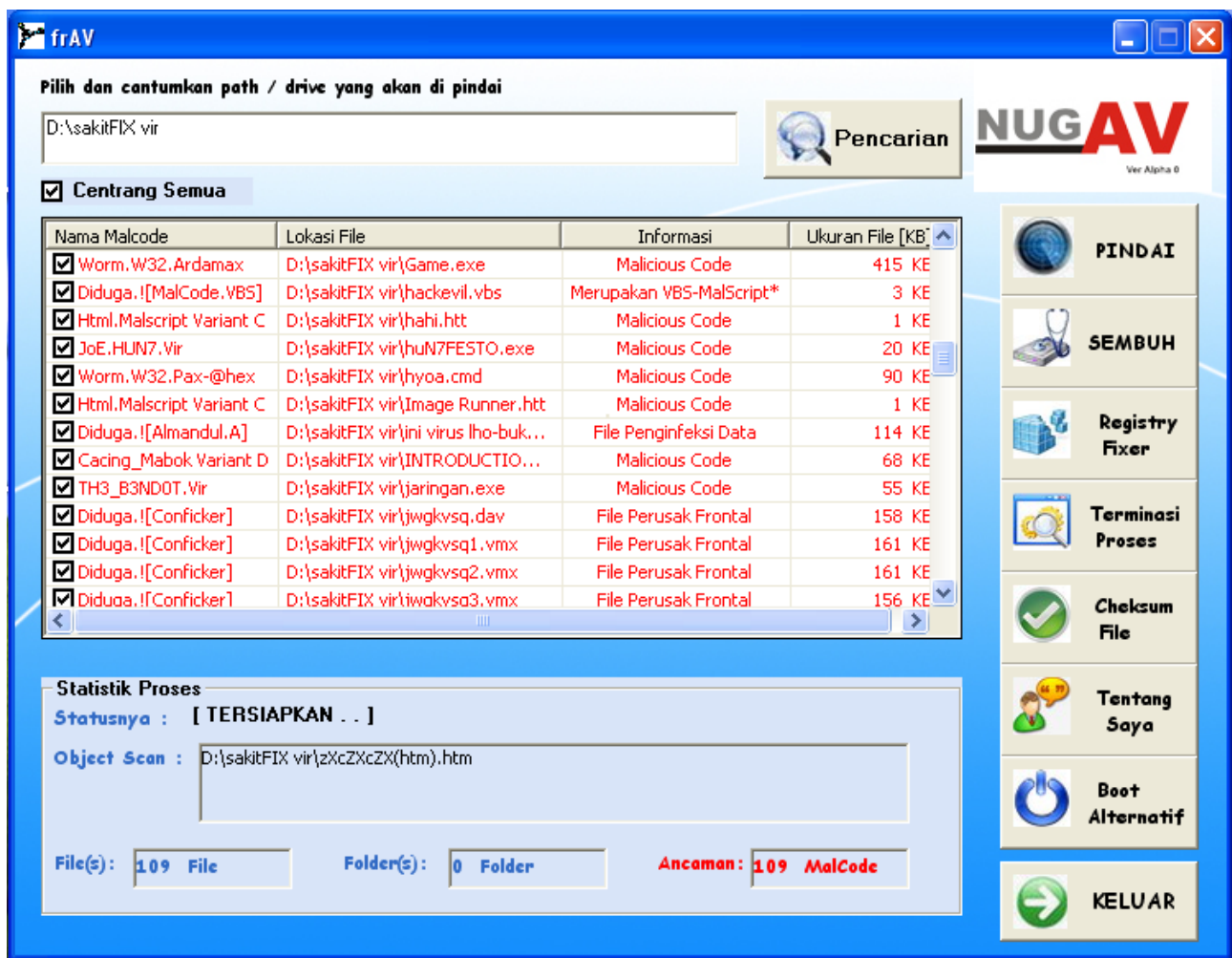
## 4. Implementasi dan Pembahasan

### 4.1 Pengujian Aplikasi Antivirus Terhadap Malcode Yang Terpapar

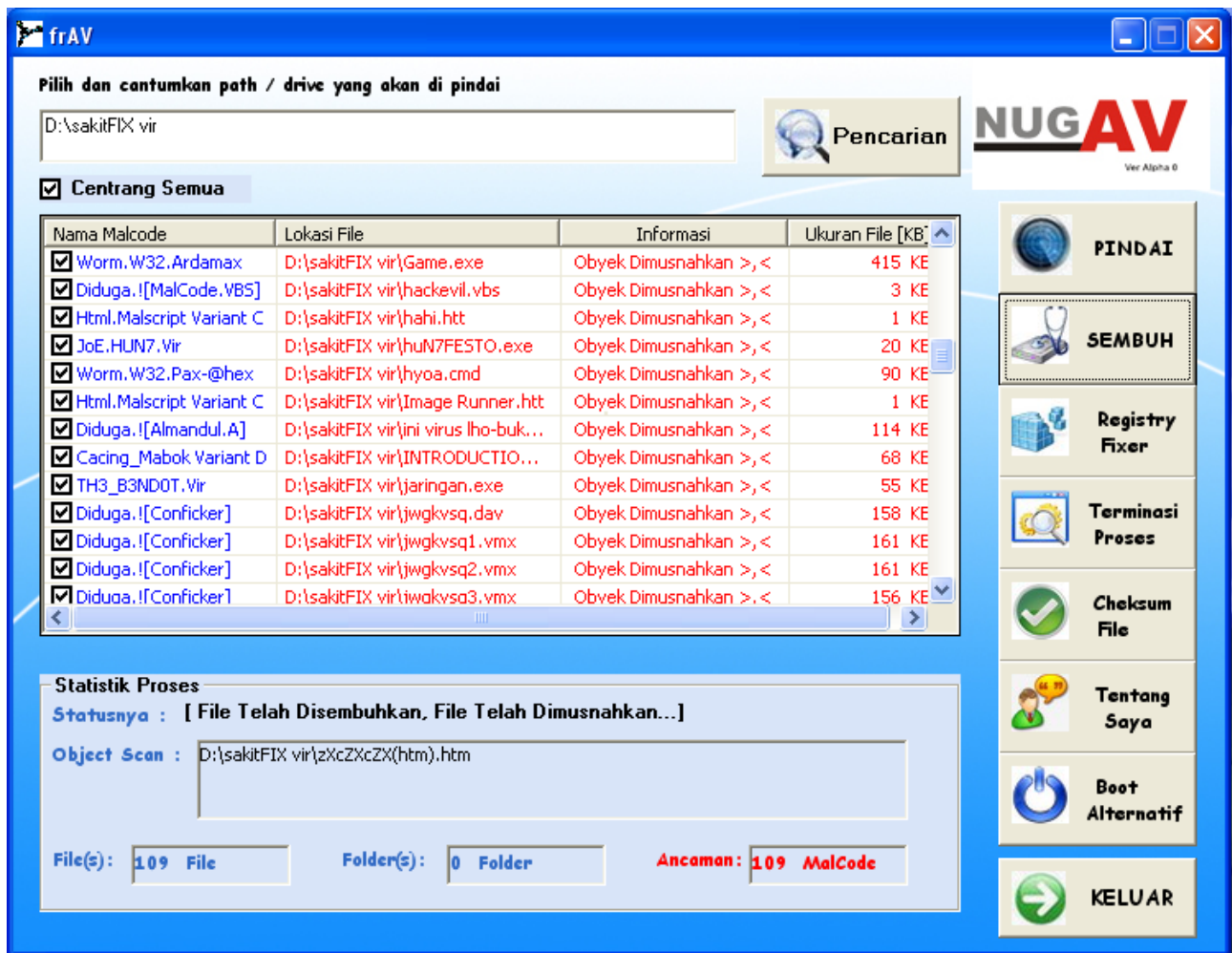
Pengujian ini dilakukan untuk memastikan bahwa sistem dapat berjalan dengan baik pada sistem operasi windows XP profesional SP2 dan berjalannya heuristik yang ditanam dalam NugAV ver Alpha 0



Gambar 14 Proses awal aplikasi dijalankan (Loading)



Gambar 15 Proses penjarangan malcode dalam komputer dan berjalannya heuristik



**Gambar 16** Proses penyembuhan file dokumen yang terinfeksi dan pemusnahan malcode

## 5. Kesimpulan

Kesimpulan pokok mengenai Aplikasi Pertahanan Terhadap Serangan Malcode Dalam Sistem Operasi Microsoft Windows XP Profesional SP2 yang dapat diambil dari uraian penjelasan dan pembahasan pada bab sebelumnya antara lain:

1. Aplikasi antivirus memerlukan database atau signature malcode untuk mendeteksi nama malcode yang beredar untuk menjaringnya dan mengeksekusi malcode tersebut.
2. Malcode atau tepatnya suatu file memiliki karakter yang berbeda satu sama lainnya, agar bisa di baca oleh mesin atau computer, karakter ini yang disebut nilai Hexadecimal (*Hexadecimal value*), untuk mendapatkan nilainya aplikasi ini menggunakan standar M31 Pattern.
3. Pendeteksian suatu malcode tidak hanya dengan signature malcode berdasarkan Hexadecimalnya, karena jika suatu file yang terinfeksi yang diambil sampel maka kemungkinan salah deteksi besarnya 50-70%, oleh karena itu penanaman heuristik



diberlakukan agar lebih akurat dalam menjaring malware karena menggunakan string karakter malware itu sendiri.

4. Penggunaan API (*Application Programming Interface*) dicanangkan untuk memudahkan kinerja antivirus itu sendiri dikarenakan API adalah suatu kode rekomendasi langsung dari pembuat system operasi windows untuk menjelajahi, mengeksplorasi, dan memanipulasi system tersebut.
5. Proses pemindaian(*scanning*) didasarkan atas signature malware dan heuristik, yaitu mendeteksi nilai Hexadecimal terlebih dahulu setelah cocok maka nama malware akan ditampilkan, namun jika suatu file tidak ada kecocokan dengan signature maka heuristik diberlakukan disini untuk dicocokkan string karakternya.
6. Hasil yang diberikan berupa nama malware, alamat malware tersebut berada, ukuran filenya, keterangan tambahan, dan proses eksekusi serta pembenahan segera dilakukan.

### **Daftar Pustaka**

- Administrator, 2009, Programming, <http://www.programminglearn.com/category/database>, Tutorial Database, diakses 28 Maret 2010
- Download Virus & Software, 2009, Virus, <http://morphians.wordpress.com/download-virus-software/>, Virus, diakses 11 Januari 2010
- Download Source Code, 2009, Source, <http://morphians.wordpress.com/download-source-code/>, Source, diakses 11 Januari 2010
- Forum, 2009, Antivirus, <http://codenesia.com/smfforum/index.php/board,28.0.html>, Signature, Hexadecimal, diakses 12 Desember 2009
- Forum, 2009, Virus <http://codenesia.com/smfforum/index.php/board,16.0.html>, Source Code Virus, Virology, diakses 12 Desember 2009
- Hirin, A.M. 2008. Sehari Menjadi Programmer AntiVirus Menggunakan VB 6.0. Yogyakarta: ANDI Publishing
- Hörz.Maël, 2009, FreeWare Programs, Products <http://mh->

[nexus.de/en/downloads.php?product=HxD](http://nexus.de/en/downloads.php?product=HxD), HxDen (*Hex Editor and Disk Editor*), diakses 11 November 2009

Madiun. MADCOM. 2005. Aplikasi Pemrograman Database dengan Visual Basic 6.0 dan Crystal Report. Yogyakarta: ANDI Publishing

Madiun. MADCOM. 2003. Database Visual Basic 6.0 dengan SQL. Yogyakarta: ANDI Publishing

Microsoft, 2004, Microsoft Support, <http://support.microsoft.com/default.aspx?scid=kb;en-us;187913>, How To List Running Processes, diakses 11 November 2009

Microsoft, 2004, Shell, <http://support.microsoft.com/search/default.aspx?query=shell&catalog=LCID%3D1033&mode=r>, Use ShellExecute, diakses 11 November 2009

Microsoft, 2004, Taskkill, <http://support.microsoft.com/search/default.aspx?query=taskkill&catalog=LCID%3D1033&mode=r>, Utility to end a service process, diakses 11 November 2009

Microsoft, 2004, API(*Application Programming Interface*), <http://support.microsoft.com/search/default.aspx?mode=r&query=API&spid=global&catalog=LCID%3D1033&1033comm=1&ast=25&ast=28&res=20>, How To Use the Registry, diakses 11 November 2009

Permata.F, 2007, TutorialVisualBasicScript, <http://wss-id.org/blogs/fadh325/archive/2007/06/19/Mudah-Menguasai-Visual-Basic-Script.aspx>, Mudah Menguasai Visual Basic Script, diakses 21 Maret 2010

Prasetyo, Didik, D. 2006. 101 TIP & TRIK Visual Basic 6.0. Jakarta: Elex Media Komputindo Kelompok Gramedia

Russinovich.Mark, 2010, Process Utilities, [http://technet.microsoft.com/id-id/sysinternals/bb896653\(en-us\).aspx](http://technet.microsoft.com/id-id/sysinternals/bb896653(en-us).aspx), ProcessExplorer, diakses 21 Februari 2010

Russinovich.Mark and Cogswell.Bryce, 2009, Process Utilities, [http://technet.microsoft.com/id-id/sysinternals/bb963902\(en-us\).aspx](http://technet.microsoft.com/id-id/sysinternals/bb963902(en-us).aspx), AutorunsViewer, diakses 21 Februari 2010

Saputra, J. 2005. EKSPLORASI KEKUATAN WIN32-API dengan Visual Basic. Jakarta: Elex Media Komputindo Kelompok Gramedia

Selftaught, 2005, GUI (*Graphic User Interface*), <http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=62937&lngWId=1>, vbComCtl revisited, diakses 28 Maret 2010

Sunyoto, A. 2006. Pemrograman Database dengan Visual Basic dan Microsoft SQL. Yogyakarta: ANDI Publishing

Wikipedia, 2008, API, [http://en.wikipedia.org/wiki/Application\\_programming\\_interface](http://en.wikipedia.org/wiki/Application_programming_interface), API Functions, diakses 15 April 2010