

# Metode Sederhana Mematikan Proses Aplikasi yang menggunakan teknik UNICODE

**Edwin Pelleng**

*Ewin9k@gmail.com*

*http://ewin74.blogspot.com*

## ***Lisensi Dokumen:***

*Copyright © 2003-2010 IlmuKomputer.Com*

*Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.*

Seperti diketahui banyaknya virus lokal yang beredar membuat banyak programmer yang terdorong untuk membuat antivirus. Para VirusMaker yang tidak mau virusnya terbunuh, berusaha membunuh AntiVirus duluan.

Karena itu AntiVirusMaker mulai mengembangkan berbagai teknik, salah satunya adalah dengan menggunakan UNICODE. UNICODE sendiri adalah standar baru yang lebih pengkodean yang lebih canggih dari standar lama yaitu ASCII. Kebanyakan sekarang virus lokal yang sebagian dibuat dengan VB6 tidak mendukung UNICODE secara default maka tidak bisa mendeteksi kehadiran ANTIVIRUS yang menggunakan UNICODE untuk di kill prosesnya.

Namun fokus utama tulisan ini bukanlah tentang cara membuat virus, melainkan teknik sederhana yang bisa digunakan untuk mengkill proses meskipun aplikasi killer tersebut, misalnya sebuah program malware tidak mendukung UNICODE.

## **Pendahuluan**

Disini saya akan membahas teknik mengkill aplikasi yang menggunakan UNICODE sebagai anti identification, karena sebagian program menerapkan perbandingan nama untuk mengidentifikasi nama proses untuk diambil PID.

PID inilah yang digunakan untuk mengkill proses, yaitu dengan menghandle proses tersebut.

## **Isi**

Dalam proses search and destroy, biasanya suatu process manager akan scanning biasanya virus akan mencoba membandingkan nama proses dengan daftar nama yang sudah ada sebelumnya. Namun sebuah program yang tidak mendukung standar UNICODE yang mencoba menscan

proses maka tidak akan mampu mendapatkan nama file tersebut.

*Perhatikan Contoh Berikut:*

Sebuah Aplikasi yang menggunakan nama: **AntiVirus.exe**

Ketika akan discan yang tampil hanyalah: ?ntiVirus.exe

Terus bagaimana cara mengidentifikasi? Sederhana saja!

Tinggal periksa saja apa nama aplikasi tersebut memiliki karakter ? (tanda tanya), karena bisa dipastikan bahwa karakter tersebut adalah UNICODE. Untuk melakukan itu tinggal gunakan berbagai fungsi misalnya dalam Bahasa C dan FreeBASIC bisa menggunakan StrStr, dalam VB bisa menggunakan InStr dan dalam Delphi bisa menggunakan Pos. Berikut adalah beberapa contoh:

FreeBASIC

```
#Include Once "windows.bi"
#include Once "win/tlhelp32.bi"
#include Once "crt/string.bi"

Sub CariHancurkan()
    Dim hSnapShot As HANDLE
    Dim nProcess As BOOL
    Dim uProcess As PROCESSENTRY32
    Dim buff As ZString*64
    Dim hProses As HANDLE

    hSnapShot = CreateToolhelp32Snapshot(2, 0)
    uProcess.dwSize = Len(uProcess)
    nProcess = Process32First(hSnapShot, @uProcess)
    Do While nprocess
        If (InStr(UCase(uProcess.szExeFile), "?")>0) Then
            hProses = OpenProcess(PROCESS_TERMINATE,0,uProcess.th32ProcessID)
            TerminateProcess(hProses, 0)
            Print "======"
            Print "[[UNICODE DIDETEKSI]]"
            Print "EXE: "+ Str(uProcess.szExeFile)
            Print "PID: "+ Str(uProcess.th32ProcessID) + " --> TEWAS!!!"
            Print "======"
            EndIf
            nProcess = Process32Next(hSnapShot, @uProcess)
        Loop
    End Sub

'////////////////////////////////////

Print "Anti UNICODE"
Print "======"
Print
CariHancurkan()
Print
Print "Tekan sembarang untuk melanjut..."
Do While InKey$="":Loop
```

C++ (Tested in VC++ 6.0)

```
// AntiUnicode.cpp : Defines the entry point for the console application.
//

#include "stdafx.h"
#include <windows.h>
#include <stdio.h>
#include <tlhelp32.h>
#include <string.h>

void judul()
{
    printf("AntiUnicode Proses\n(c)2010 Edwin Pelleng\n\n");
}

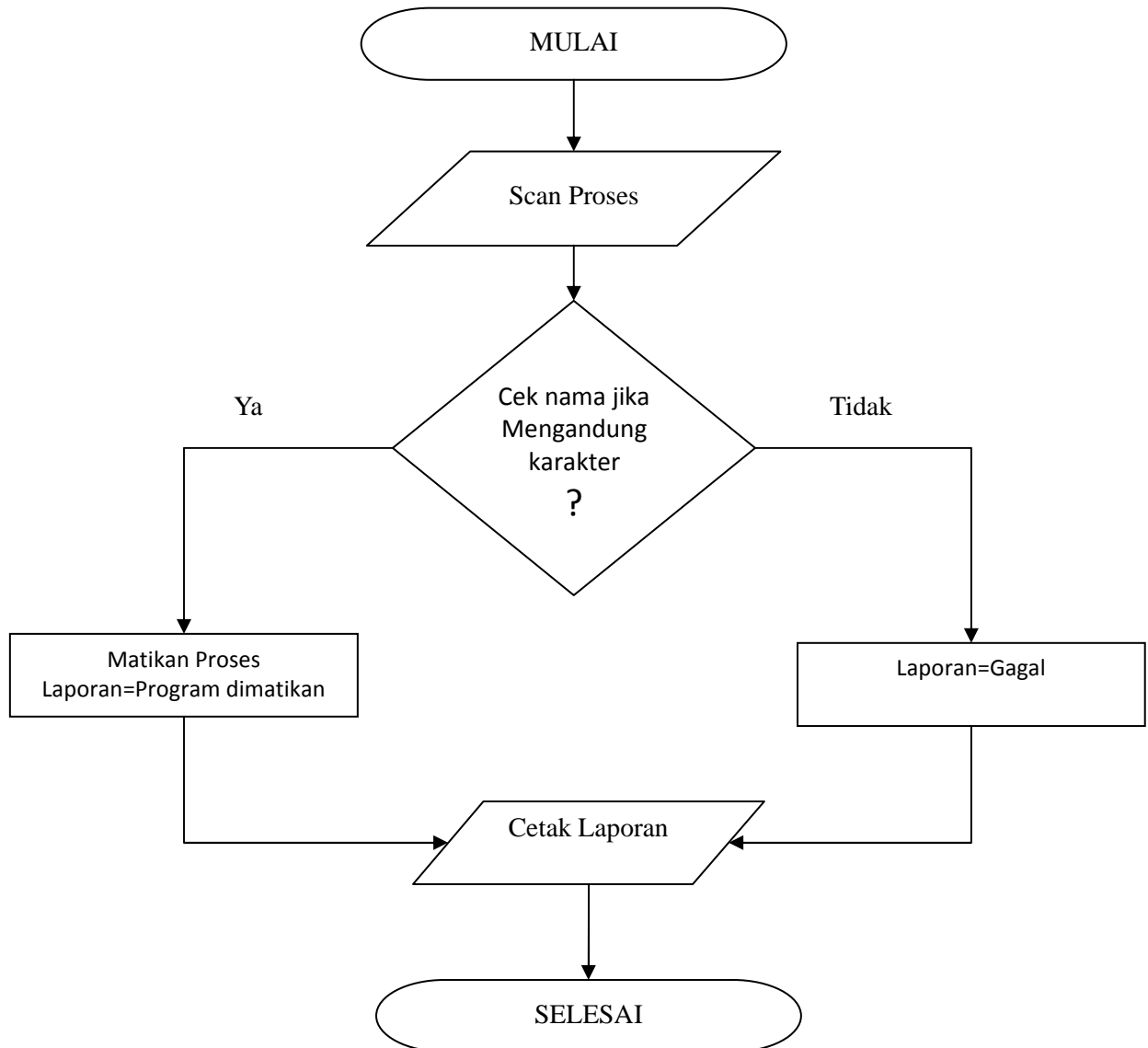
void carihancurkan()
{
    HANDLE hPSnap, hProses;
    PROCESSENTRY32 uProcess;
    char buff[MAX_PATH];

    memset(&uProcess, 0, sizeof(uProcess));

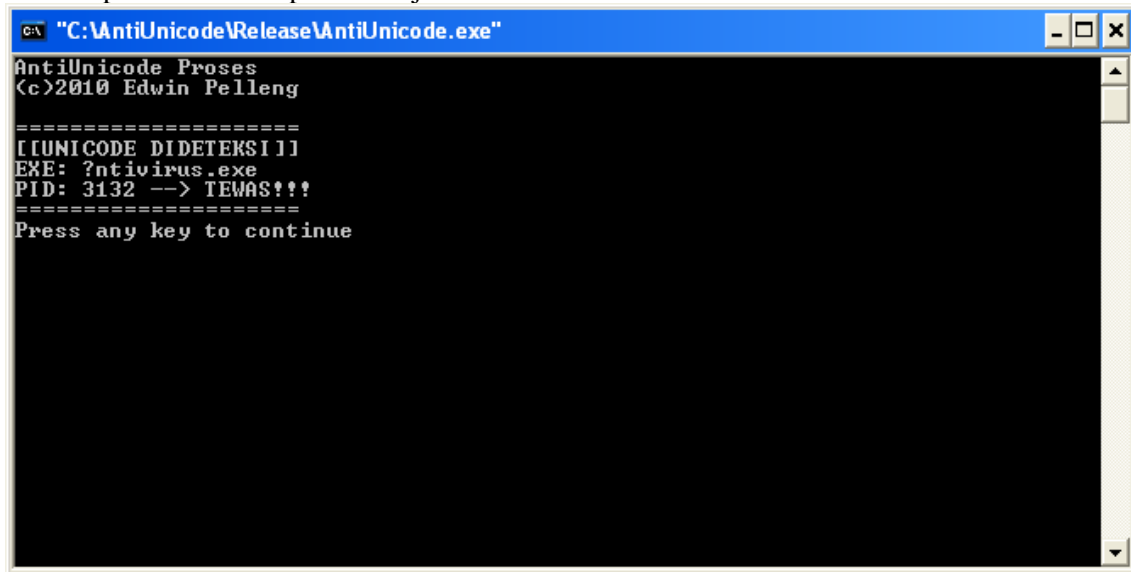
    hPSnap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    uProcess.dwSize = (DWORD) sizeof(PROCESSENTRY32);
    if (Process32First(hPSnap, &uProcess) != 0)
    {
        do
        {
            strncpy(buff, uProcess.szExeFile, sizeof(buff));
            if (strstr(buff, "?")){
                hProses = OpenProcess(PROCESS_TERMINATE, 0, uProcess.th32ProcessID);
                TerminateProcess(hProses, 0);
                printf ("=====\n");
                printf ("[[UNICODE DIDETEKSI]]\n");
                printf ("EXE: %s\n", uProcess.szExeFile);
                printf ("PID: %d --> TEWAS!!!\n", uProcess.th32ProcessID);
                printf ("=====\n");
            }
        }
        while (Process32Next(hPSnap, &uProcess) != 0);
    }
    (void) CloseHandle(hPSnap);
}

int main(int argc, char* argv[])
{
    judul();
    carihancurkan();
    return 0;
}
```

Logika adalah sebagai Berikut



Jika script di atas dicompile dan dijalankan maka:



```
"C:\AntiUnicode\Release\AntiUnicode.exe"
AntiUnicode Proses
<c>2010 Edwin Pelleng

=====
[[UNICODE DIDETEKSII]
EXE: ?ntivirus.exe
PID: 3132 --> TEWAS!!!
=====
Press any key to continue
```

Bagaimana dengan VB & Delphi?

Saya tidak membuat contoh Visual Basic karena scriptnya mirip dengan script FreeBASIC karena menggunakan InStr. Silahkan anda modifikasi saja sendiri. Demikian juga dengan pengguna Delphi bisa menggunakan fungsi Pos. Logikanya sama, yaitu jika ditemukan karakter ? dalam nama proses maka proses tersebut akan dikill.

## Biografi Penulis

**Edwin Pelleng.** Sementara Kuliah S1 di Prodi Pend. Teknik Informatika, Fakultas Teknik, UNIMA.