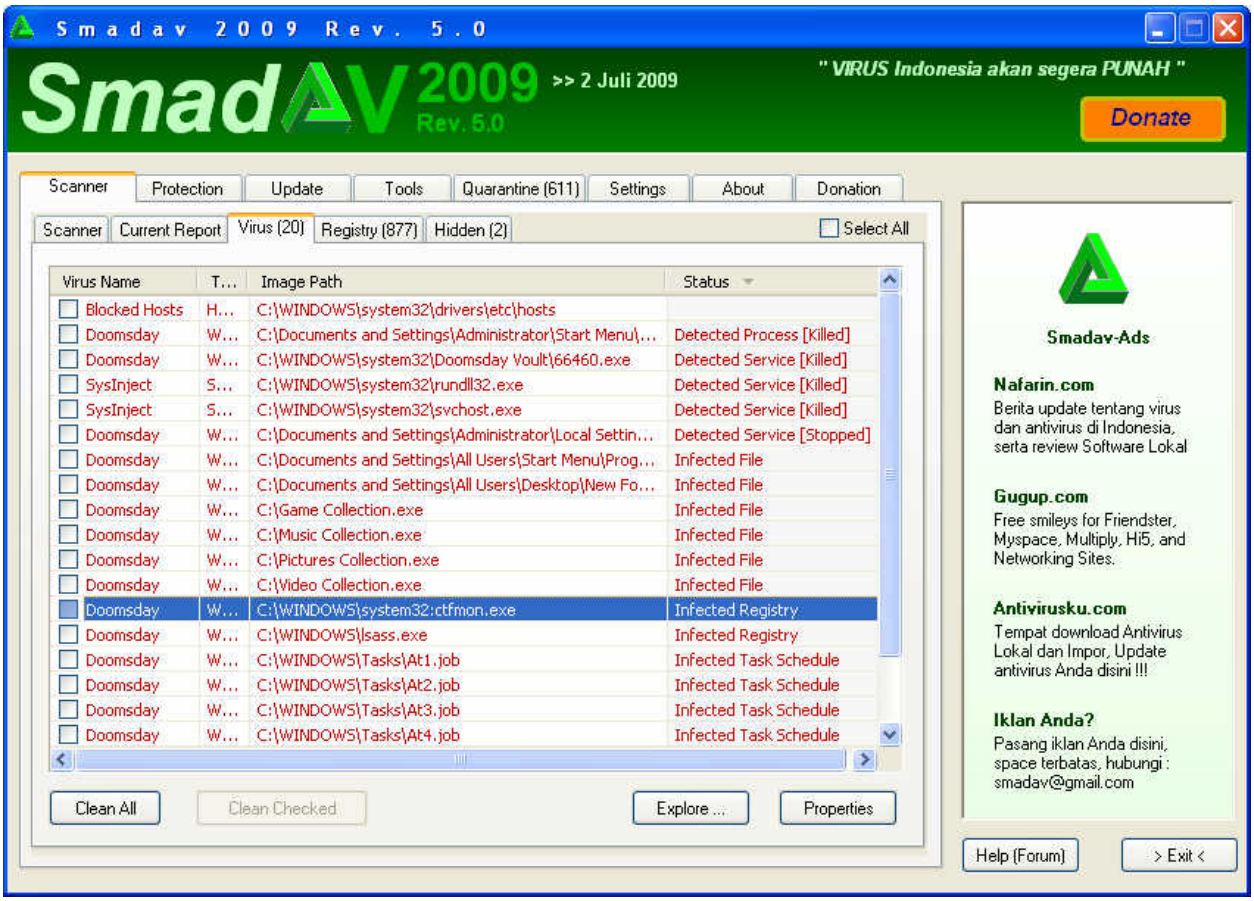
NAMA : ACHMAD HADI PRAYOGA
NIM : 1310651188
KELAS : C

NO. 2

CARA MEMBERSIHKAN VIRUS DOOMSDAY dengan SMADAV

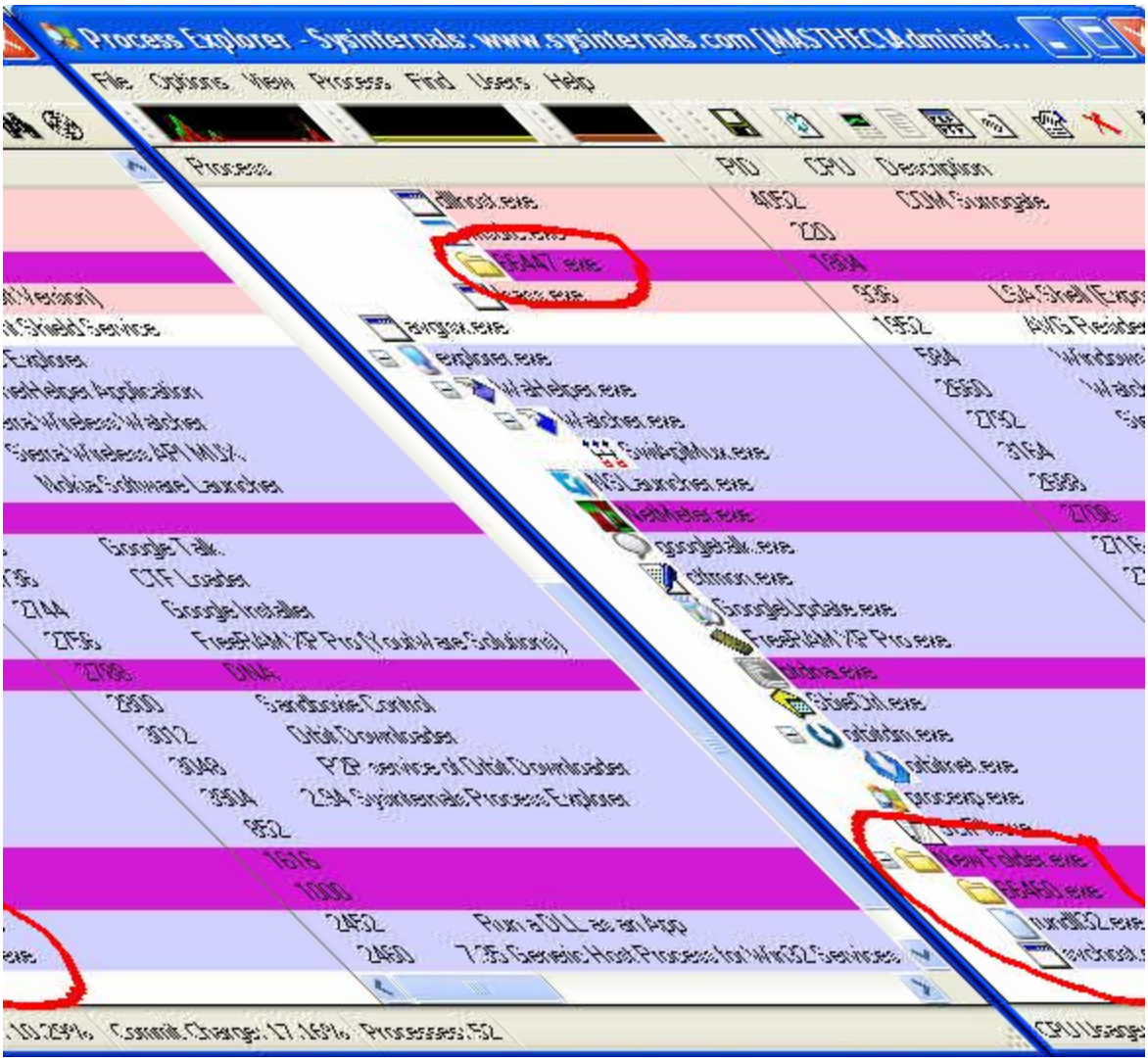


Virus Doomsday adalah virus yang dibuat oleh salah seorang pakar virus Indonesia dengan tujuan sebagai promosi bukunya yang membahas tentang pemrograman virus. Disamping itu, tujuan lainnya yaitu untuk menantang kekuatan antivirus lokal Indonesia untuk membersihkan virus ini sampai tuntas. Tujuan ini sangat bagus sehingga para tim antivirus lokal bisa memperbaiki engine dan teknik antivirusnya agar bisa membunuh virus ini. Apakah Anda setuju dengan adanya buku pemrograman virus? Mudah-mudahan saja buku tersebut lebih banyak manfaatnya dibanding ruginya, dan mudah-mudahan juga buku canggih itu tidak dimanfaatkan pembuat virus lokal untuk membuat virus lokal yang lebih canggih lagi, karena kita harapkan sebentar lagi virus lokal akan punah

Virus Doomsday ini sangat sulit dihapus dengan cara manual karena menggunakan hampir semua teknik virus lokal yang pernah ada dan ditambah lagi dengan teknik-teknik baru yang ditambahkan oleh pembuatnya. Itulah mengapa pembuatnya memberi nama Doomsday untuk virus ini, karena dia mengira antivirus lokal tidak akan mampu membasminya. Tapi, Smadav 2009 Rev. 5 mudah saja membunuh virus ini sampai ke akar-akarnya sehingga komputer yang terinfeksi sebelumnya akan kembali seperti semula seakan-akan belum pernah terinfeksi virus ini. Pembersihan ini sangat cepat, tidak lebih dari 15 detik setelah satu kali klik Smadav.

Sebelum membersihkan virus ini dengan Smadav, mari kita bahas dulu apa saja kecanggihan virus ini.

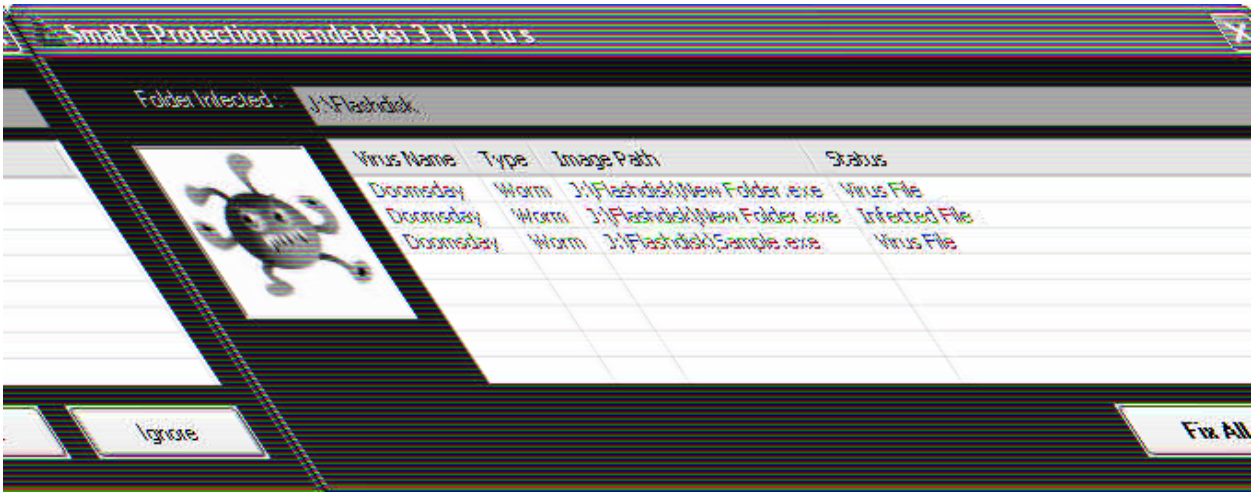
Virus ini dibuat dengan Visual Basic 6 dikompresi dengan UPX dan mempunyai ukuran 65 KB. Jika dilihat di Process Explorer, disana terlihat ada 5 proses virus yang sedang aktif. 1 proses yang paling atas aktif sebagai Windows Service dan tugasnya adalah untuk mencegah kita membuka tool system di windows seperti regedit, msconfig, dll. Sedangkan kumpulan 4 proses yang paling bawah yang punya tugas utama untuk melakukan penyebaran dan pertahanan di komputer korban. 4 proses ini saling melindungi satu sama lain, jika kita membunuh salah satu prosesnya maka proses lain akan kembali menghidupkan proses yang kita bunuh tadi, jadi kita akan kesulitan jika membunuhnya secara manual dengan process explorer seperti ini. Walaupun berhasil, semua proses ini akan kembali aktif kalau kita membuka program apa saja di komputer kita. Jadi kita harus memperbaiki registry dulu untuk membersihkannya, tapi registry pun diblok dengan teknik berlapis-lapis. Jadi, hampir tidak mungkin virus ini bisa diberantas dengan cara manual karena selain sulitnya membunuh proses di memori, virus ini juga merusak sangat banyak value registry.



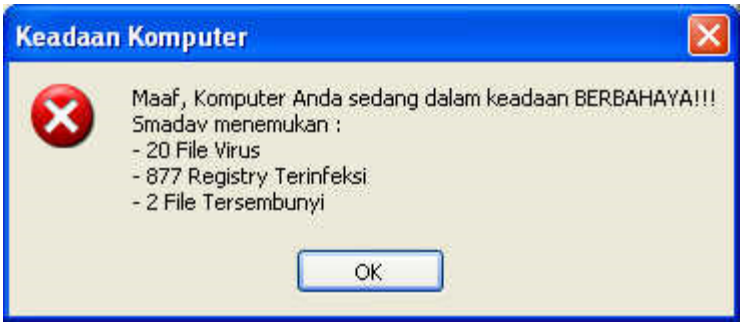
Virus ini akan memblok semua akses ke antivirus lokal (PCMAV, SMADAV, atau ANSAV), hampir semua antivirus impor, dan program-program lain yang bisa membahayakan dirinya. Dia mempunyai teknik yang sangat banyak dan cerdik untuk mengenali dan mencegah program yang membahayakannya. Tapi dia tidak mampu untuk mengenali Terupdate, sehingga Smadav Terupdate bisa dengan mudah menghancurkannya. Selain memblok program,virus ini juga akan memblok akses ke situs antivirus.

Sekarang mari kita lihat hasil scan Smadav.

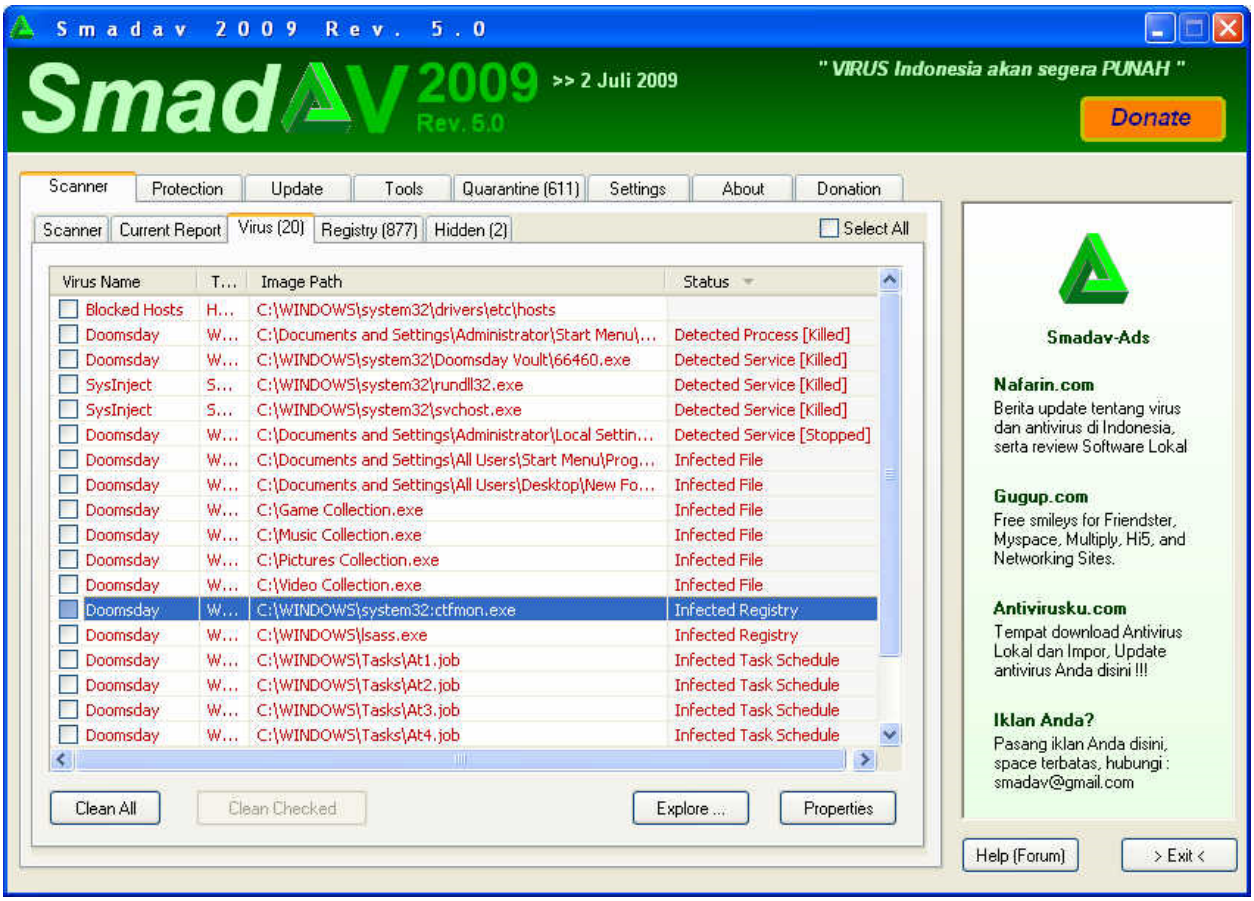
Kalau folder pada komputer/flashdisk yang teinfeksi Doomsday diakses lewat windows explorer maka SmaRTP akan muncul segera memperingatkan bahwa ada virus dan harus segera dihapus. Ini screenshot-nya :



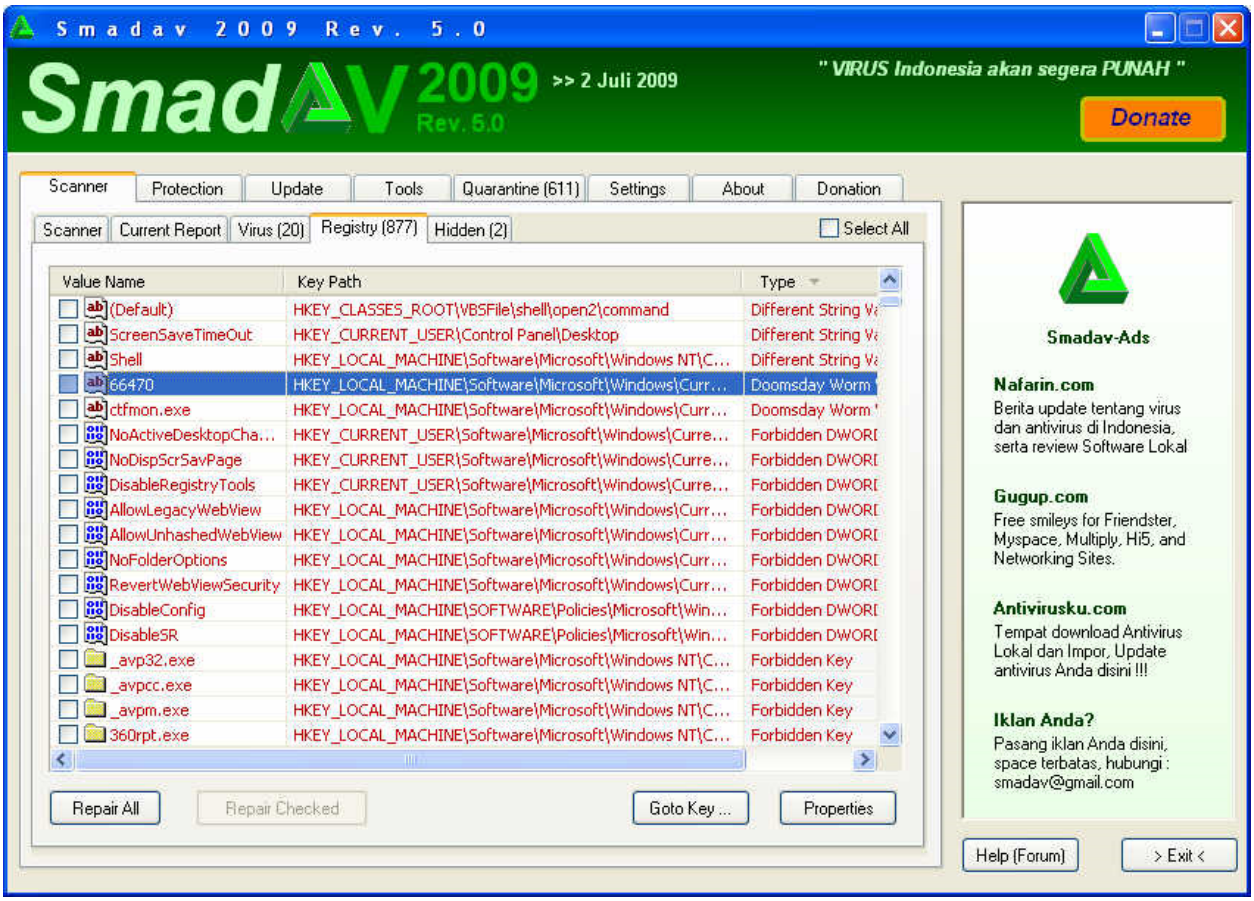
Setelah membuka Smadav Terupdate pada komputer yang terinfeksi Virus Doomsday, maka Smadav akan segera memperingatkan bahwa ada virus yang aktif di komputer sehingga scanning akan otomatis dimulai. Setelah menunggu beberapa detik, scanning akan selesai dan memperlihatkan hasil seperti screenshot ini :



Kemudian kita bisa melihat-lihat bahwa banyak sekali file virus yang terdeteksi dan registry yang rusak. Ini screenshot file virus yang terdeteksi :



Dan di bawah ini screenshot registry yang terinfeksi, disana terlihat Smadav mendeteksi 877 value registry yang rusak, ini didapatkan setelah Smadav melakukan scanning pada lebih dari 2000 value registry :



Kemudian klik saja Fix All dan tunggu beberapa detik lagi sampai semuanya sudah hilang, lakukan scanning ulang dengan mode full scan (scanning keseluruhan) pada komputer untuk mendeteksi file-file virus yang sudah mati yang masih tersisa di komputer.