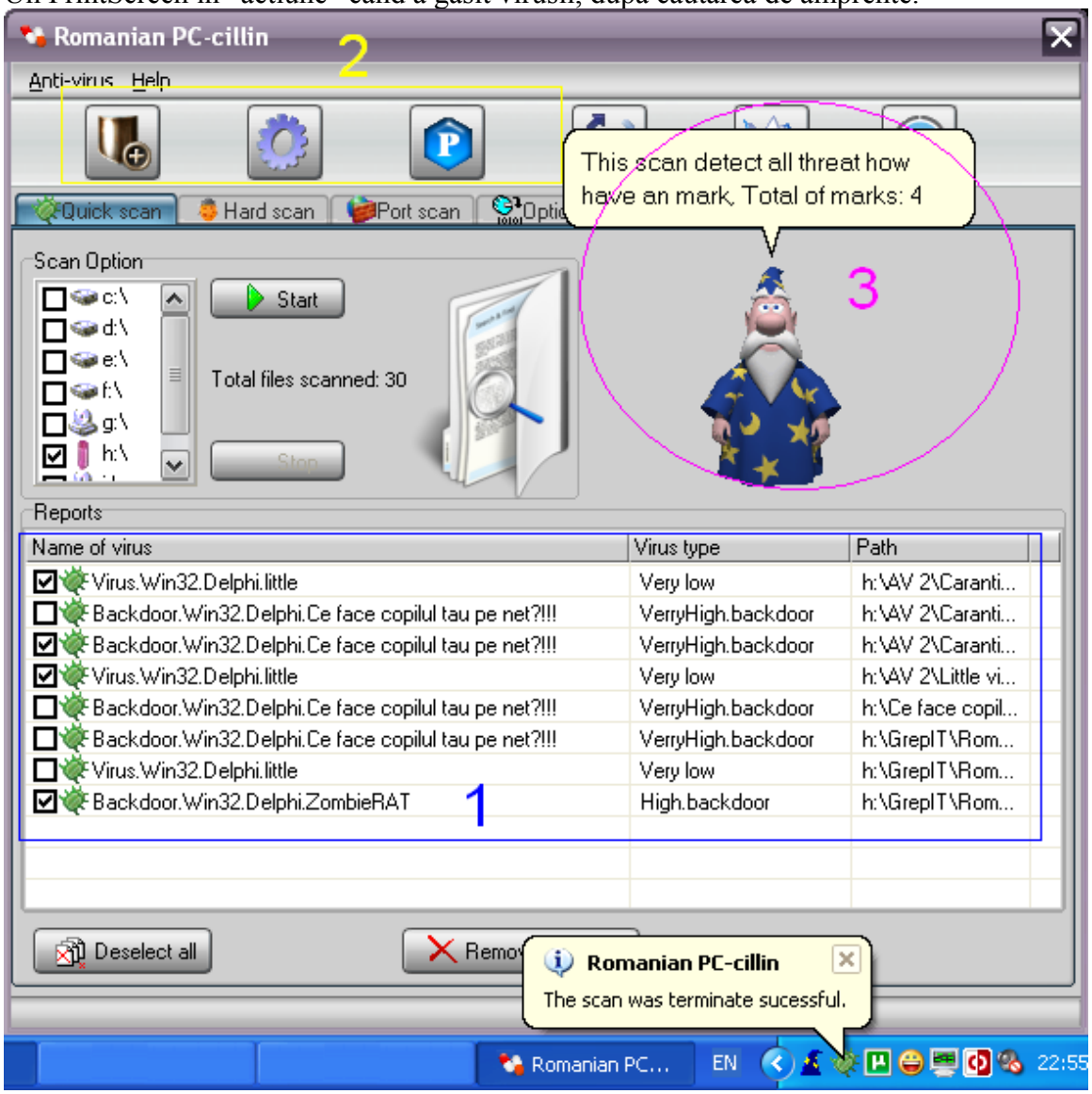
Romanian PC-Cillin

Version 1.5

Este o aplicatie, care ma bantuie de foarte mult timp, pana la urma m-am hotarat sa o scriu, documentandu-ma am inteles ca domeniul anti-virus, este un domeniul vast, complet dinamic existand cel putin 80.000 de virusi windows cu amprente cunoscute(deci acesti au dezasamblati si pentru fiecare s-a scris un cod de dezinfectie, si s-a studiat comportamentul fiecaruia).

Un PrintScreen in “actiune” cand a gasit virusii, dupa cautarea de amprente.



Legenda:

1. Virusi detectati dupa scanarea cu amprente.
2. Meniul secundat, si meniul principal
3. Helpul dinamic(Merlinul)

Ce este?

Romanian PC-Cillin este un mic anti-virus, care detecteaza coduri malitioase, in urma scanarilor fisierelor(.exe, .com., .bat) si o analiza simpla a porturilor. Cuprinde si un micut “Computer repair”, cu mici coduri de reparare a sistememului de operare, si un hexa-editor care permite vizualizarea si scrierea locatiilor de memorie a unor fisiere.

Observatie!

Hexa-Editorul nu realizeaza, conversiunea din hexa in octocod(codul ASM, al CPU 8086)

Cum functioneaza?

Detectand amprente cunoscute, sau detectand virusi chiar si fara amprente, Cum?

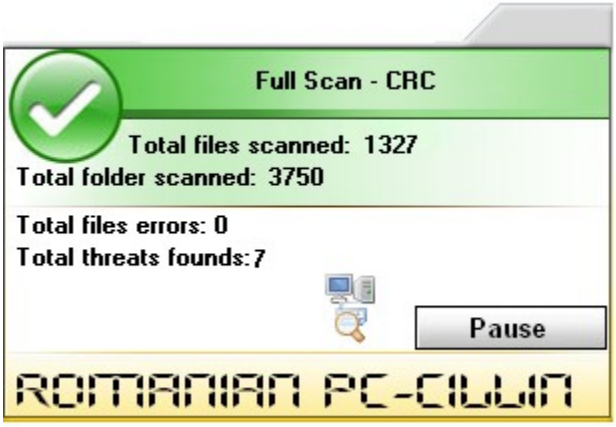
1. Urmarind stabilitatea fisierelor in timp.
2. Cautand fisiere care si-au modificat structura initiala.
3. Virusi(backdoor-uri) care deschide anumite porturi(conexiuni).
4. Auto-Protection scanner, verifica daca anumite configuratii sunt corecte precum:
    i. Windows Firewall – on,
    ii. Task Manager – enable
    iii. RegEdit – enable

- Deoarece exista foarte multi virusi, care afecteaza aceste componente ale sistemului de operare.

Scanarile

Cum am mentionat mai sus, programul are 4 tipuri de scanari

1. Scanare dupa amprente
   - Avand amprenta, cautam fisierele pitite(virusii),
2. Scanare dupa modificare de CRC
   - Avem CRC-urile la toate (*.exe;*.com*.bat) si verificam periodic daca si-au modificat valorile in timp, adica si-au modificat structura(lucru nepermis)
3. Scanare dupa anumite porturi
   - Scanam porturile deschise calculatorului, pe baza unor tabele, “ Virusi porturi”
4. Verificarea periodic automat, a unor componente ale sistemului de operare, pentru securitate. Iar daca sunt dezactivate, anti-virusul avertizeaza utilizatorul, de problema si programul permite reactivarea lor.



A se vedea un printscreen cu CRC - scan

In urma scanarilor, fisierele(virusii), pot fi trecuti in carantina, ulterior se poate lua decizia dea fi sterse. Pe parcursul programului, am folosit termenul dezinfectie, lucru neadevarat, intr-un cat dezinfectia inseamna NU a sterge ci a recupera programul, fara virusi. Programul nu face asta, doar sterge fisierul infectat(il muta in carantina, stergand-ul din folderul original), deci programul NU permite corectia erorilor, NU au utilizatorul methode de corectie a erorilor.

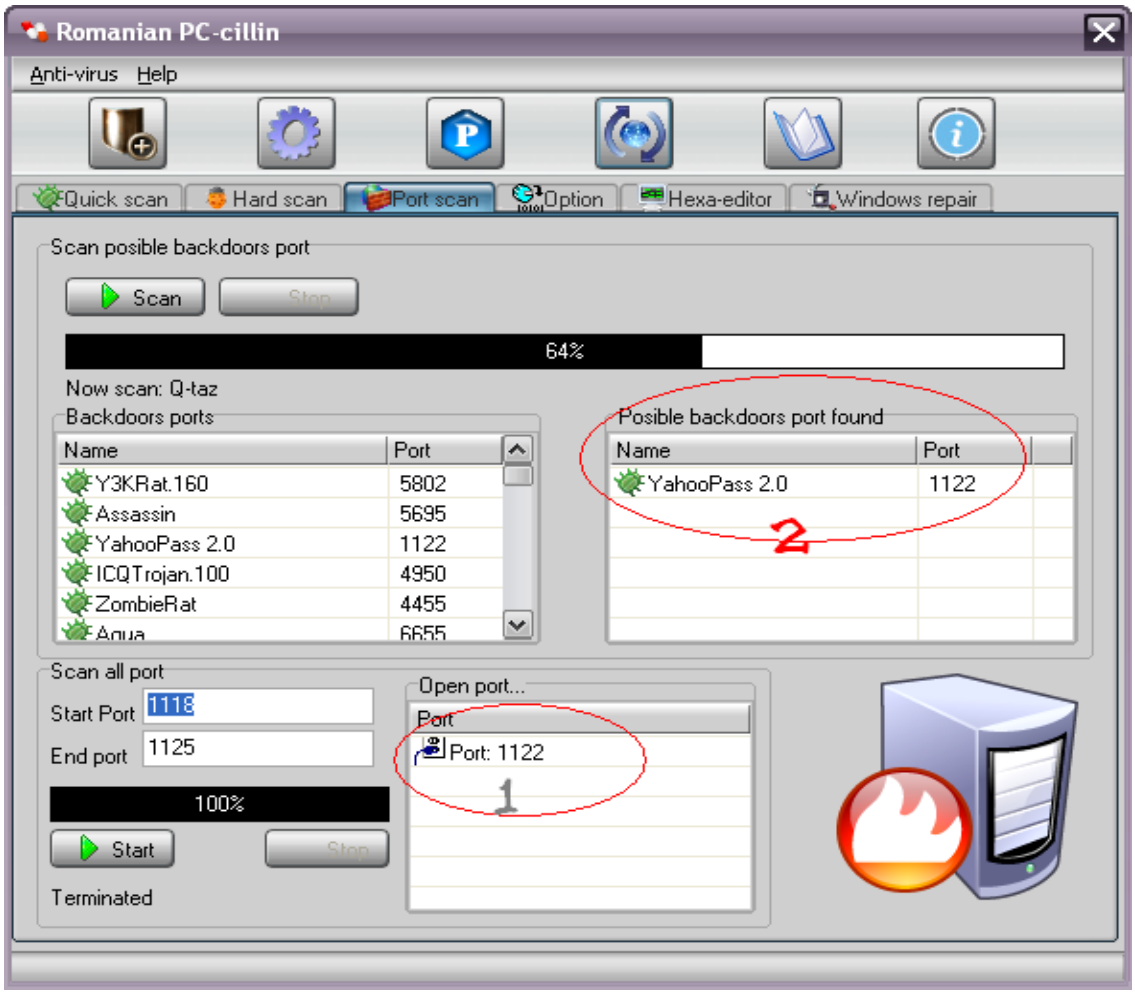
Port scan

Programul are posibilitatea de a scana selectiv intervale de porturi, sau de a scana porturi deschide de virusi cunoscuti(backdoor-uri)

Ex de tabel „Virusi porturi”

Nume backdoor	Portul
Bionet	12348
ZombieRAT	4455
YahooPass v 2.0	1122
SubSeven	6712
Metal	19604
Scarb	1255
Masakker	7119

Un PrintScreen cu panoul la „Port-scan



Legenda: 1 – Reprezinta porturile deschise din intervalul 1118 – 1125(deci portul deschis este 1122, la mine in calculatorul, in momentul respectiv)

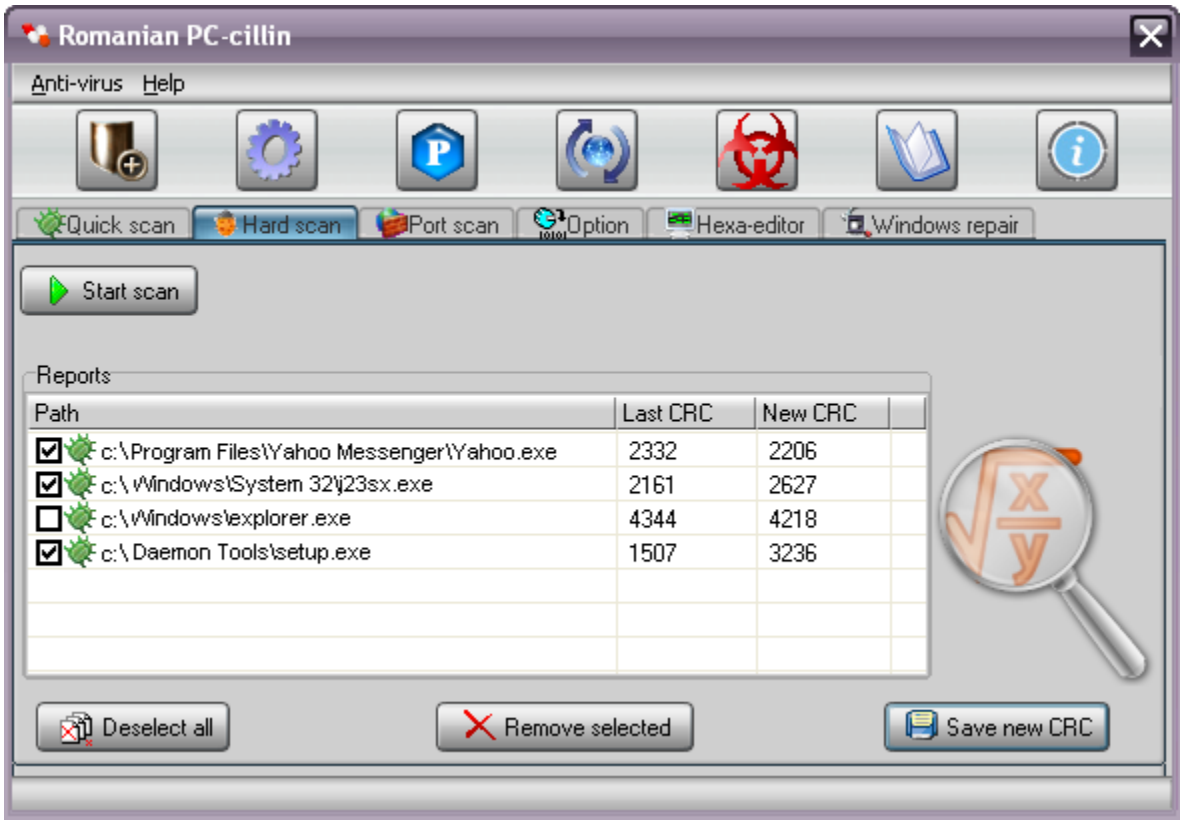
2 – Reprezinta posibilele backdoor-uri gasite dupa scanarea de porturi.

NOTA: Nu am scris cod de verificarea corespondentei intre port si programul respective, adica faptul ca am gasit portul gasit, am considerat ca am gasit si virusul

CRC

Cum am mentionat mai sus, programul poate sa detecteze virusi a caror amprenta este necunoscuta, sau necatalogata inca. Aceasta modalitatea permite determinarea oricarui virus a caror manifestare modifica programele (*.exe, *.bat, *.com)

Initial programul calculeaza CRC-urile la toate fisierele (*.exe, *.bat, *.com) din calculator pe baza unei formule proprii(o suma de control facuta dupa o anumita regula), le stochez intr-un fisier(CRC.crc) si ulterior la o scanare se confrunta noul CRC vechi cu cel nou. Daca nu o sa fie identice, cineva a rescris executabilul. Lucru interzis.



Auto-Protection system

Este o facilitate a programului, sa detecteze configuratii arormale ale calculului utilizatorului, si putand sa avertizeze utilizatorul si sa le corecteze automat. Aceastea sunt:

- Windows Firewall – off
- Windows Task Manager –disable
- Windows Registry Editor - disable

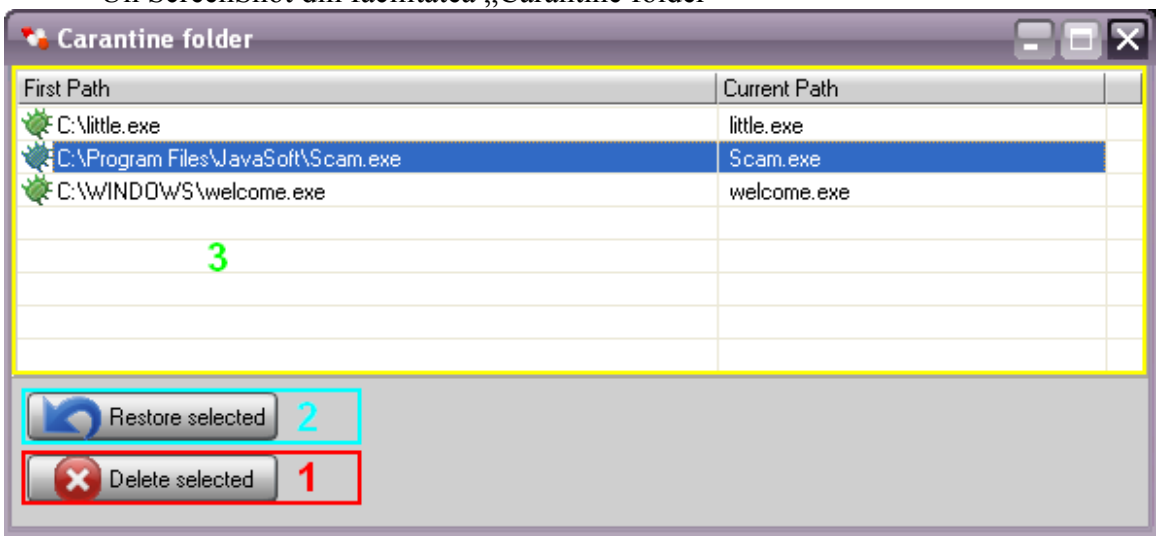
Carantine folder

Este o facilitate a programului care permite, stocarea fisierelor suspecte, avand capacitatea:

1. De a-le sterge; stergere definitiva;
2. Sau restaurarea lor in pozitia initiala(First Path)

Restaurarea se face cu fisierul in acelasi stadiu, adica fisierurul nedezinfectat (nedevirusat)

Un ScreenShot din facilitatea „Carantine folder”

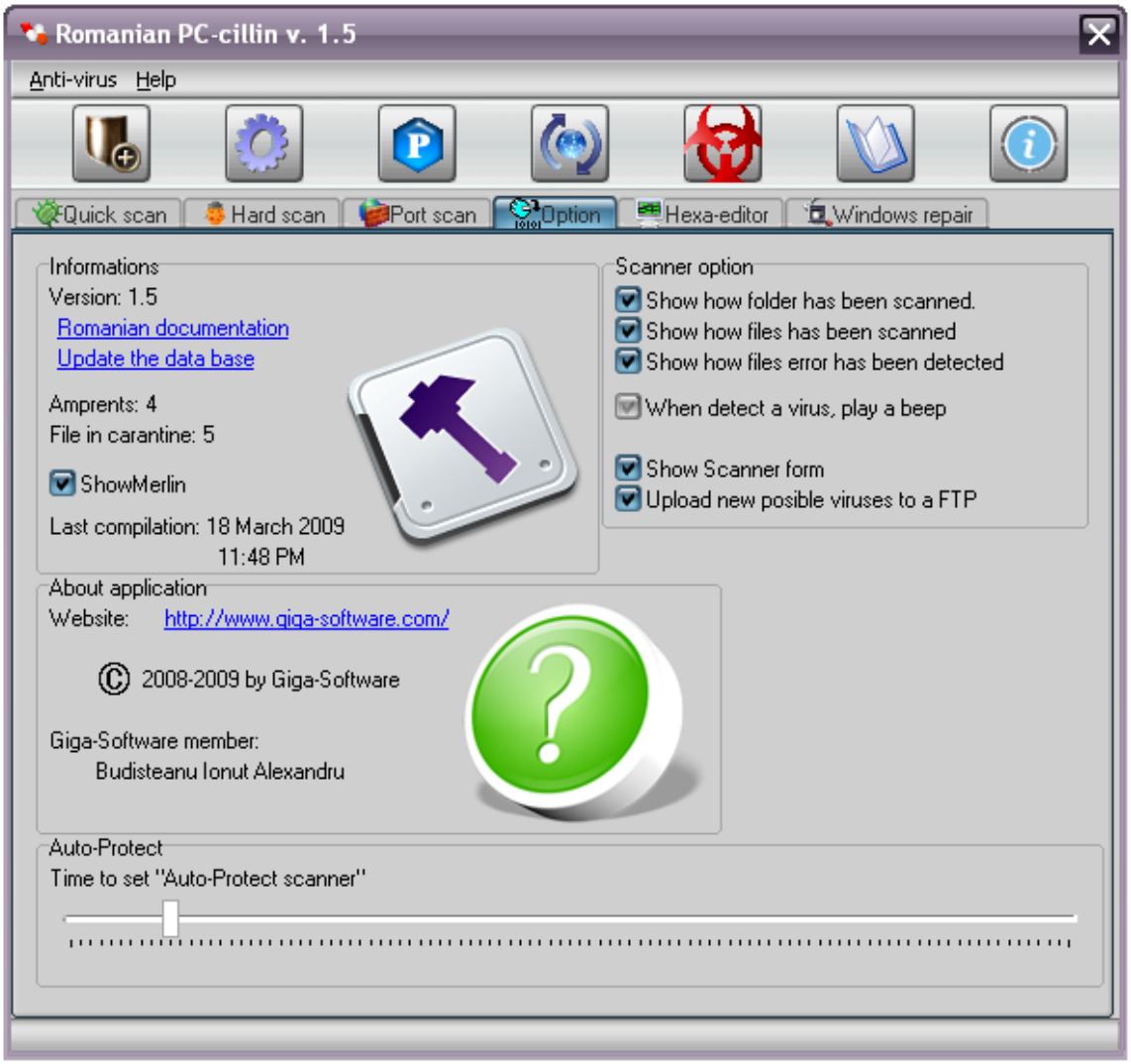


Legenda: 1. Stergerea fisierului definitiv

2. Restauarea fisierului, in pozitia initiala(First Path)
3. Programele care sunt puse in carantina(adica copiate in folderul „Carantine”(ProgramPath+’\Carantine\’)

Options

Programul poate fi configurat dupa optiunile utilizatorului. Ele se salveaza, si data viitoare cand utilizatorul va deschide softul, se configureaza automat. Se salveaza in ProgramPath+'info.cfg')



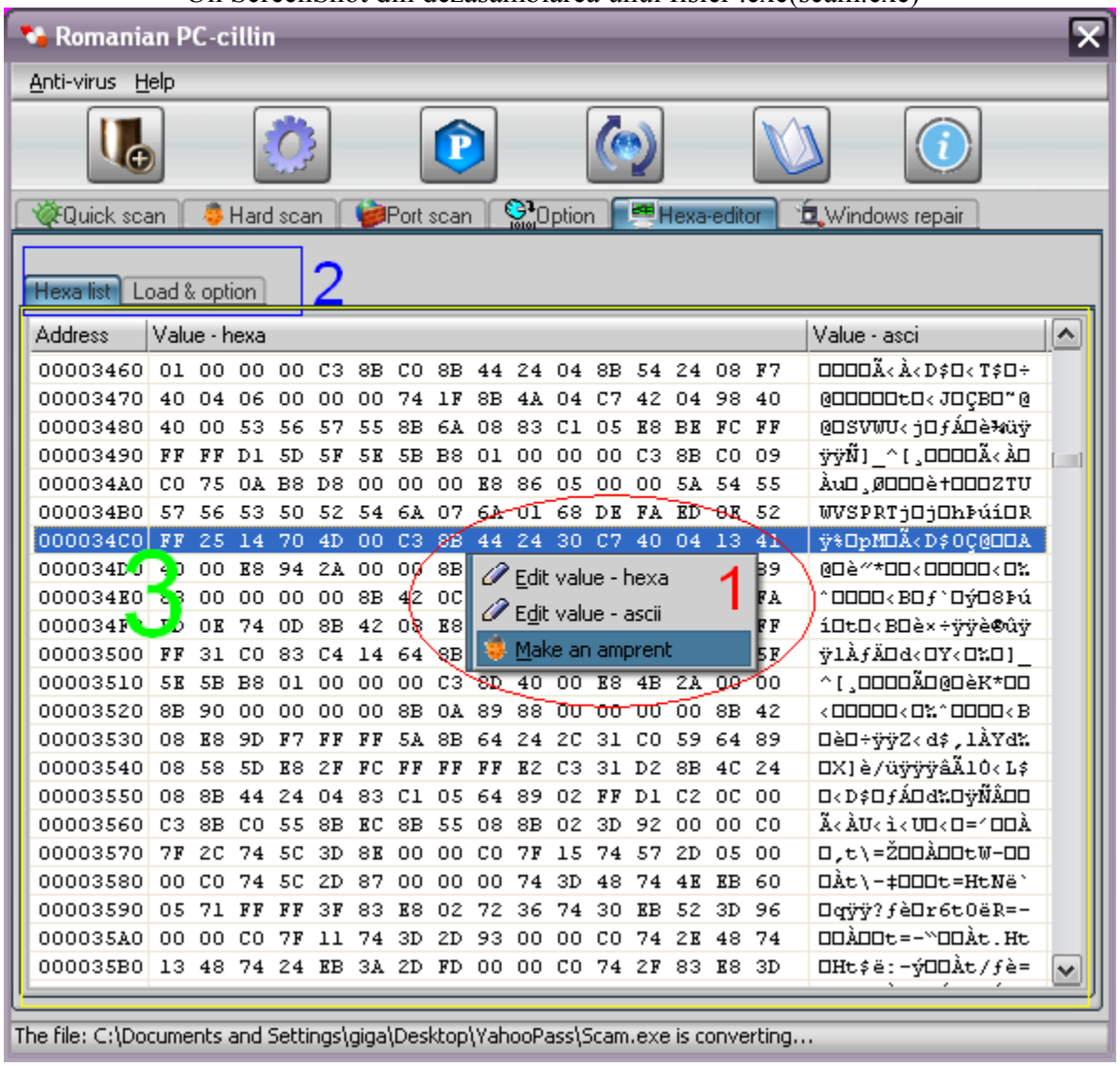
Hexa-Editor

Hexa-Editorul este tool care permite vizualizarea continutul unui fisier(orice extensie) in format hexa-zecimal si ASCII.

Permite editatea conctinutul locatiilor(hexa sau ASCII)

Aceasta parte a programului permite si crearea amprentelor. Mentionez inca o data, ca programul nu realizeaza dezasamblarea, negenerand codului in ASAMBLOR(octocod)

Un ScreenShot din dezasamblarea unui fisier .exe(scam.exe)



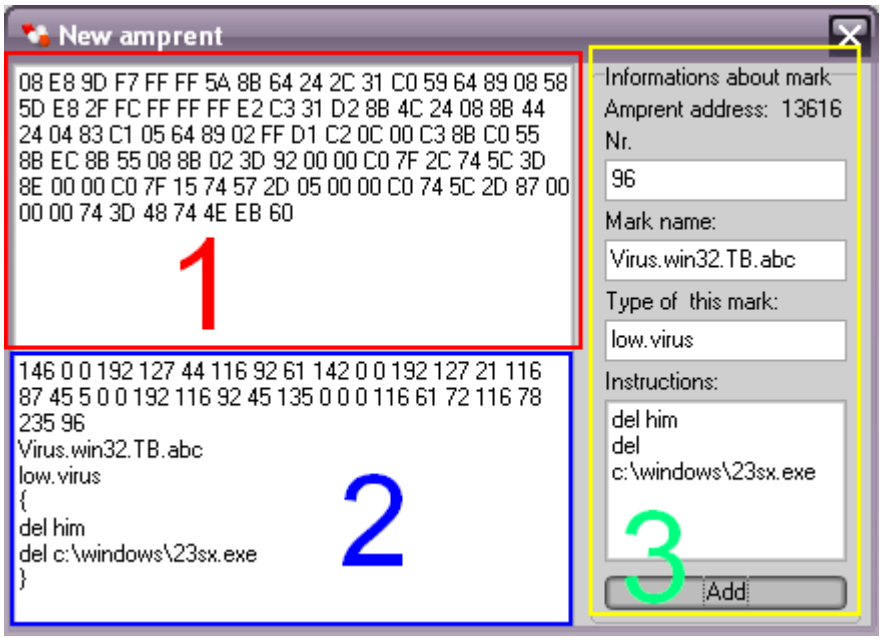
Legenda: 1 – Submeniul hexa-editorului

2 – Meniul hexa-editorului

3 – Aplicatia scam.exe dezasamblata

Creare amprente

Un ScreenShot din „Make new amprent”



Legenda: 1. Adresele amprentei
2. Salvarea amprentei in formatul anti-virusului(cum ar arata amprenta)
3. Informatii despre amprenta.

Observatii

La realizarea programului, am urmarit doar aplicarea unor concepte, si nu optimizarea codului respectiv, adica:

- Am utilizat CD-KEY (Un serial este: b!m-5Q[-?D3-z$1)
- Programul permite scanarea concurenta.
- Programul are 4 clase de threaduri diferite.
- Programul face upgrade dupa server la baza de date, pastrand in acest fel legatura programatorului cu programele. Deci nu este un program izolat, deci este un program distribuit
- Are un help, dinamic, fiind Merlin si Leo, care ghideaza utilzatorul pe parcursul utilizarii programului.
- Curpinde si un Windows Repair, tinand cont ca foarte multi virusi, blocheaza task-mangerul, inchide procese, etc...
- Programul cuprinde un creator de amprente in care orice utilizator, poate creea amprente si le poate cauta in calculator.
- Programul permite trimiterea fisierelor care si-au modificat structura(adica dupa scanarea CRC-urilor), pentru a fi anilizate pe un server, la „sediul” programatorului, trimiterea se face prin intermediul FTP

- Are un sistem de administrare a carantinei.
- Calculeaza CRC-ul fisierelor, dupa o anumita formula proprie, este o simpla suma de control facuta pentru viteza... se pot aplica diversi algoritmi mai complicatii
- Permite scanarea partiala, a calculatorului(si stickuri sau alte device-uri) in cautarea de amprente digitale. Permite si scanarea partitilor virtuale(exemplu, partitie create cu programul Daemon tools)
- La realizarea programului am utilizat skinuri, si custom skin. Formurile neregulate(cele care nu sunt patrate; care au bitmapuri ca si background, si au zimturi pe margini) sunt programate de mine, deci bilioteca de skinuri nu. Icon-urile sunt luate din diverse surse. NU am considerat util, a avea un partener designer, doar pentru a-mi desena niste iconuri.
- Nu am folosit alte componente care nu sunt in paleta standard, infara de skin;
- Am utilizat un Active-X(fiind MSAgent 2.0), fiindu-mi necar pentru agenti „Leo” si „Merlin”, am utilizat si functii ale OS-ului(functii standard din win32 SDK), exemplu la taskmanager...
- Programul a fost dezvoltat in mediul vizual „Borland Delphi 6.0”, durata de creare este de 60+ zile. S-au realizat 5 versiuni.

M-am orientat catre acest program, care in stadiul in care se gaseste era bun daca era scris acum 7 ani.

Bibliografie:

1. Pentru intelegerea fenomenelor virus/anti-virus http://vx.netlux.org/lib/aps00.html#cf6 , cea mai buna carte de virusi/anti-virusi pe care am gasit-o