ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 130379 A2**

(51) Int.Cl.
G06F 21/00 (2006.01);
G06F 21/55 (2013.01);
G06F 21/56 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2013 00848**

(22) Data de depozit: **29.03.2012**

(30) Prioritate:
16.05.2011 US 13/068610

(41) Data publicării cererii:
30.06.2015 BOPI nr. **6/2015**

(86) Cerere internaţională PCT:
Nr. **EP 2012/055733 29.03.2012**

(87) Publicare internaţională:
Nr. **WO 2012/156143 22.11.2012**

(71) Solicitant:
• **F-SECURE CORPORATION**,
TAMMASAARENKATU 7, PL 24, HELSINKI, FI

(72) Inventatori:
• **TURBIN PAVEL**, *C/O F-SECURE CORPORATION, TAMMASAARENKATU 7, PL 24, HELSINKI, FI*

(74) Mandatar:
ROMINVENT S.A.,
STR. ERMIL PANGRATTI NR.35, SECTOR 1, BUCUREŞTI

(54) # EXPLORARE PENTRU SOFTWARE RĂU INTENŢIONAT CU CĂUTARE ÎN AVANS

(57) **Rezumat:**

Invenţia se referă la o metodă de explorare, în vederea depistării unui software rău intenţionat (engl. malware), în timpul execuţiei unei aplicaţii pe un sistem de calculator. Metoda conform invenţiei cuprinde: detectarea, de către aplicaţie, a accesărilor fişierelor din cadrul unui director comun, utilizarea accesărilor detectate, pentru a identifica unul sau mai multe grupuri de fişiere, din cadrul directorului comun menţionat, care pot fi accesate ulterior de aplicaţie, şi explorarea acelui unu sau mai multe grupuri de fişiere, pentru depistarea software-ului rău intenţionat, înainte ca aplicaţia să încerce să acceseze fişierele grupului sau grupurilor.

Revendicări: 22
Figuri: 7

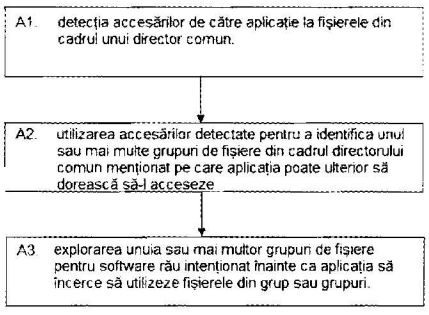

Fig. 4

RO 130379 A2

Domeniul Tehnic

Invenția prezentă se referă la o metodă și un aparat pentru efectuarea de explorare pentru software rău intenționat (eng. malware). În particular, invenția prezentă se refera la o metodă și un aparat pentru optimizarea performanței unui sistem de calculator care efectuează explorare pentru software rău intenționat pe un grup de fișiere.

Fondul Invenției

În limba engleză termenul Malware este prescurtarea de la software rău intenționat (eng. malicious software) și este utilizat ca un termen pentru a se face referință la oricare software proiectat pentru a infiltra sau a deteriora un sistem de calcul fără consimțământul în cunoștință de cauză al proprietarului. Software-ul rău intenționat poate include virusuri de calculator, viermi, cai troieni, kituri de rădăcină (eng. rootkits), software de reclamă (eng. adware), software de spionaj și oricare alte tipuri de software rău intenționat sau nedorit.

Numeroși utilizatori finali utilizează software anti-virus pentru a detecta, și posibil pentru a elimina software-ul rău intenționat. Cu scopul de a detecta un fișier de software rău intenționat, software-ul anti-virus trebuie să aibă o modalitate de a-l identifica dintre toate celelalte fișiere prezente pe un dispozitiv. În mod tipic, acest lucru necesită ca software-ul aniti-virus să aibă o bază de date care să conțină „semnături" sau „ amprente" care sunt o caracteristica a fișierelor de program de software rău intenționat individuale. Atunci când un furnizor al software-lui anti-virus identifică o nouă amenințare de software rău intenționat, amenințarea este analizată și semnătura acesteia este generată. Software-ul rău intenționat este apoi „cunoscut" și semnătura sa poate fi distribuită la utilizatorii finali ca actualizări la bazele de date de software anti-virus locale ale acestora.

Software-ul anti-virus în mod tipic furnizează explorarea fișierelor la cerere în care utilizatorul unui sistem de calculator determină când ar trebui să fie explorate fișierele de pe sistemul de calculator pentru detecția prezenței software-lui rău intenționat. În explorarea la cerere utilizatorul poate activa procesul de explorare în mod manual, sau poate configura procesul de explorare pentru a începe în anumite circumstanțe. De exemplu, utilizatorul ar putea configura software-ul anti-virus ca să exploreze dosare (eng. folders) sau directoare (acești termeni vor fi utilizați aici în mod interschimbabil) o dată pe săptămână, și să exploreze toate fișierele de pe un sistem de calculator o singură dată pe lună. Suplimentar, software-ul anti-virus poate de asemenea furniza protecție în timp-real împotriva software-ului rău intenționat prin efectuarea de explorare la acces.

În explorarea la acces un sistem de calcul este monitorizat pentru prezența de software rău intenționat prin explorarea fișierelor în mod automat în fundal atunci când există un acces detectat al fișierelor de către una sau mai multe aplicații care execută pe sistemul de calculator. Cea mai obișnuita metodă de acces la fișier este accesul de deschidere de fișier numai pentru citire. Acest tip de acces este comun pentru operațiuni pe fișiere multiple, de exemplu la căutarea pentru/în fișiere, la pornirea și în timpul execuției unei aplicații, la copierea fișierelor de la dosar la dosar (director la director), la comprimarea de fișiere, etc. Următoarele exemple ilustrează suplimentar unele dintre aceste operațiuni obișnuite.

Exemplul 1, comanda copy (copiere):

C:\>copy source.* d:\dest*

Această comandă (aplicație) ar putea fi reprezentată de către următorul pseudo cod:

pentru fiecare fișier din c:\ source.**

deschide numai pentru citire fișierul curent (c:\ source\...)

citește datele din fișier
închide fișierul
salvează datele la d:\dest

Comanda de copiere generează acces numai pentru citire continuu și secvențial pentru toate fișierele sursă.

Exemplul 2, o aplicație care execută cu mai multe fișiere de modul:

Se presupune faptul că aplicația constă dintr-un singur executabil (.EXE) și un număr de module cum ar fi biblioteci legate în mod dinamic (dynamic linked libraries - .DLL). Atunci când un utilizator lansează aplicația, aplicația încarcă bibliotecile necesare și apoi începe execuția. Această operațiune ar putea fi reprezentată de către următorul pseudo-cod:

pentru fișierele application.exe, module1.dll, module2.dll ... moduleN.dll
deschide numai pentru citire fișierul curent
încarcă datele din fișier

Aplicația generează accesări de deschidere de fișier numai pentru citire continue și secvențiale pentru fișierele sursă din aplicație și/sau directoarele de modul relevante.

Modele similare de acces de deschidere de fișier numai pentru citire continuu și secvențial de fișiere multiple dintr-un director dat pot fi găsite în alte comenzi sau aplicații, de exemplu căutarea unui model într-o colecție de fișiere (*grep.exe* sau *findstr.exe*), calculul unui șir de octeți de comprimare (eng. hash) peste fișiere (*md5.exe*), împachetarea într-un container (*rar.exe* sau *winzip.exe*) și așa mai departe.

Figura 1 ilustrează o interacțiune obișnuită între o aplicație și software anti-virus atunci când aplicația efectuează un acces de deschidere de fișier numai pentru citire de fișiere multiple. În timpul operațiunii numai atunci când software-ul anti-virus detectează accesul de către aplicație la fișiere acesta efectuează explorarea la acces a fișierelor.

În particular, atunci când aplicația încearcă să deschidă un fișier, solicitarea de deschidere este interceptată de către un filtru care generează o solicitare de explorare pentru utilizare de către software-ul anti-virus și împiedică aplicația sa deschidă și să utilizeze fișierul. La recepția solicitării de explorare, software-ul anti-virus explorează fișierul și generează un rezultat în modalitatea obișnuită. În dependență de rezultat, accesul fișierului este înmânat înapoi la aplicație pentru utilizarea sa, de exemplu, citirea, copierea, sau execuția fișierului. Cu toate acestea, dacă fișiere multiple au nevoie să fie accesate de către aplicație, această operațiune va fi repetată în mod secvențial pentru fiecare acces de fișier ulterior de către aplicație așa cum este prezentat în Figura 1. Acesta este un proces foarte lent și laborios, care impactează performanța aplicației și sistemului de calculator.

Majoritatea sistemelor de calculator moderne sunt acum optimizate pentru execuția de sarcini multiple. Un CPU tipic adesea include suport de nuclee multiple (fire multiple de execuție), care permite în mod eficient sarcinilor de aplicație să fie executate ca și cum ar apare în mod simultan. Un fir de execuție (un fir) este definit ca cea mai mică unitate de procesare (de exemplu o sarcină sau o porțiune a unei sarcini) care poate fi planificată de către un sistem de operare. Execuția de fire multiple se referă la o aplicație care are fire de execuție multiple în care firele sunt planificate pentru a fi executate de către un sistem de operare în același timp. Articolul INTEL™, „Predicția și Măsurarea Performanței Paralele" („Predicting and Measuring Parallel Performance"), 9 Martie, 2010, disponibilă de la http://software.intel.com/en-us/articles/predicting-and-measuring-parallel-performance/, descrise dezvoltarea de software paralelizat de către aplicații cu fire de execuție multiple pentru a termite acestora să proceseze un set de date dat în timp mai puțin, sau să proceseze seturi de date multiple într-un timp fix.

Un procesor unic poate efectua execuție de fire multiple prin multiplexarea prin divizare timpului a firelor de execuție (adică execuție de fire multiple) astfel încât procesorul comută contextul între diferite fire. Această comutație de context se întâmplă atât de frecvent încât utilizatorul percepe firele sau sarcinile ca și cum ar fi executate în

mod simultan sau în paralel. Pe un procesor multiplu sau un sistem de nuclee multiple, unele dintre fire sau sarcini în realitate execută la același moment de timp (în dependență de numărul de procesoare), cu fiecare procesor sau nucleu executând un fir sau o sarcină particular/particulară. Cu scopul de a obține performanță maximă, aplicațiile, atunci când sunt executate pe sistemul de calculator, ar trebui să încerce să paralelizeze ecuațiile sau sarcinile complexe ale acestora.

Explorarea în paralel a mai multor fișiere pentru software rău intenționat cu software anti-virus poate fi realizată prin planificarea în mod simultan a uneia sau mai multor fire pentru a trata procesul de explorare al fiecăruia dintre fișiere. Așa cum s-a menționat mai sus, sistemul de operare gestionează execuția firelor pe un sistem de calculator cu sarcini multiple și/sau nuclee multiple. Explorarea paralelă poate fi efectuată pe fișiere multiple într-o coadă de explorare pentru a crește performanța sistemului de calculator. Organizarea în coadă de așteptare a fișierelor accesate pentru explorarea de software rău intenționat poate utiliza puterea explorării paralele. Astfel de explorare ar putea fi efectuată de către metode de explorare la închidere asincrone. Dar, chiar și cu suportul de nucleu multiplu, explorarea paralelă la acces a fișierelor multiple pentru software rău intenționat în timpul accesului de deschidere de fișier numai pentru citire de către o aplicație este problematică. Organizarea fișierelor în cozi de așteptare pentru o explorare mai târziu paralelă sau în șarjă nu este o opțiune pentru aplicații care necesită operațiunea de acces de deschidere de fișier numai pentru citire. Acest tip de acces la fișier necesită un răspuns sincron imediat de la software-ul anti-virus pentru a permite aplicației să continue cât mai rapid posibil. Solicitările de explorare de la driver-ul (software specializat pentru acces la hardware) de filtrare la anti-virus nu pot fi organizate în coadă pentru procesare de grup viitoare deoarece software-ul anti-virus nu cunoaște fișierul următor pe care o aplicație îl va solicita.

Aplicațiile pot genera solicitări de deschidere de fișier numai pentru citire secvențiale multiple arbitrare și logica de explorare anti-virus tipică solicită ca fiecare solicitare de deschidere de fișier numai pentru citire să declanșeze un eveniment de explorare sau o solicitare pentru acel fișier. Din cauza naturii secvențiale a accesului la

fișier, logica de explorare nu poate determina care fișiere vor fi ulterior accesate de către aplicație. Acest lucru nu permite software-ului anti-virus să profite de efectuarea de explorare în șarjă sau în paralel de fișiere multiple pe sisteme de calculator moderne. Acest lucru înseamnă faptul că aplicația va avea nevoie fie să aștepte până când explorarea pentru software rău intenționat se termină pe toate fișierele înainte de a începe, fie să fie întreruptă în timpul execuției în timp ce fiecare fișier care trebuie să fie accesat este explorat. Ambele scenarii deteriorează în mod semnificativ performanța aplicației și a sistemului de calculator.

Procesul sincron de explorare la acces blochează o aplicație de la a începe sau de a întrerupe execuția aplicației până când o explorare pentru software rău intenționat pentru toate fișierele sau pentru fiecare fișier, a fost efectuată. Astfel, software-ul anti-virus împiedică execuția aplicației să progreseze, încetinind rata la care aceasta își poate îndeplini sarcinile. Acest lucru impactează performanță sistemului de calculator.

Rezumat

Un obiectiv al invenției prezente este de a furniza o metodă de efectuare a explorării pentru software rău intenționat care minimizează întârzierile introduse de către explorarea în timpul execuției aplicațiilor pe un sistem de calculator, astfel optimizând performanță sistemului de calculator.

În conformitate cu un prim aspect al invenției este furnizată o metoda de explorare pentru software rău intenționat în timpul execuției unei aplicații pe un sistem de calculator, metoda cuprinzând detecția de accesări de către aplicație la fișiere în cadrul unui director comun, utilizând accesările detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația poate ulterior să le acceseze, și explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor.

Aplicațiile concrete ale invenției furnizează faptul că acel software de anti-virus poate efectua exploatarea unui grup din multitudinea de fișiere fără nevoia de a bloca complet execuția aplicației înaintea utilizării unuia sau mai multor fișiere din grup.

Ca o opțiune, cuprinde suplimentar selecția grupului sau grupurilor de fișiere pe baza tipurilor de fișier ale fișierelor accesate de către aplicație. Selecția fișierelor de preferință include punerea în corespondență a tipurilor de fișier ale fișierelor accesate de către aplicație cu tipurile de fișier ale fișierelor din cadrul directorului comun. De preferință, fișierele din cadrul grupului sau grupurilor de fișiere sunt fișiere care necesită explorare. Metoda opțional cuprinde suplimentar identificarea unuia sau mai multor grupuri de fișiere prin adăugarea fișierului curent detectat pentru a fi accesat de către aplicație la grupul de fișiere pentru explorare atunci când fișierul curent necesită explorare.

Metoda include opțional faptul că utilizarea accesărilor detectate include pasul de determinarea a numărului de accesări detectate din cadrul directorului comun și utilizarea rezultatelor pentru a declanșa pasul de explorare a grupurilor, care sunt unul sau mai multe. De preferință, declanșarea pasului de explorare apare atunci când numărul de accesări detectate atinge un prag predeterminat. Opțional, utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere include pasul de adăugare a fișierului curent detectat pentru a fi accesat de către aplicație la un grup de fișiere atunci când pasul de explorare este declanșat. Opțional, determinarea numărului de accesări detectate include pasul de resetare a numărului de accesări detectate atunci când o prima perioadă de timp a trecut și pasul de explorare nu a fost declanșat. Opțional, metoda include pasul de terminare a explorării grupului sau grupurilor atunci când o a doua perioada de timp a trecut după ce pasul de explorare a fost declanșat.

Metoda include opțional include faptul că pasul de utilizare a accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere include pasul de întreținere a unei liste de tipuri de fișier a fișierelor detectate accesate și pasul de

identificare a unuia sau mai multor grupuri de fișiere include pasul de selecție a fișierelor pe baza listei de tipuri de fișier. Selecția fișierelor include suplimentar punerea în corespondență a listei de tipuri de fișier a fișierelor accesate de către aplicație cu tipurile de fișier ale fișierelor din cadrul directorului comun.

Ca o opțiune, pasul de detecție a accesărilor de către aplicație la fișiere din cadrul directorului comun include recepția unei solicitări de explorare pentru explorarea unui fișier accesat de către aplicație din cadrul directorului comun. Opțional, pasul de detecție a accesărilor de către aplicație la fișiere din cadrul directorului comun include detecția accesului la fișier de către aplicație și generarea unei solicitări de explorare pentru explorarea fișierului atunci când explorarea este solicitată.

În conformitate cu un al doilea aspect al invenției prezente este furnizat un program de calculator pentru explorarea pentru software rău intenționat în timpul execuției unei aplicații pe un sistem de calculator, programul de calcul cuprinzând mijloace de cod de program de calculator adaptate pentru a efectua pașii următori:

detecția accesărilor de către aplicație la fișiere din cadrul unui director comun;

utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația poate ulterior să dorească să le acceseze; și

instruirea unui explorator de software rău intenționat să exploreze unul sau mai multe grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor.

Programul de calculator poate cuprinde suplimentar mijloace de cod de program adaptate pentru a efectua explorarea unuia sau mai multor grupuri de fișiere pentru software rău intenționat.

În conformitate cu un al treilea aspect al invenției prezente este furnizat un program de calculator așa cum este schițat mai sus concretizat pe un mediu care poate fi citit de calculator.

În conformitate cu un al patrulea aspect al invenției este furnizat un sistem de calculator configurat pentru a explora fișiere pentru software rău intenționat în timpul execuției unei aplicații pe un procesor, sistemul de calculator cuprinzând o unitate de detecție pentru detecția accesărilor de către aplicație la fișiere din cadrul unui director comun, și utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația ar putea ulterior să vrea să le acceseze, și instruirea unei unități de explorare pentru explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor. Sistemul de calculator poate include suplimentar o unitate de explorare pentru efectuarea explorării grupurilor de fișiere, care sunt unul sau mai multe.

Scurtă Descriere a Desenelor

Figura 1 reprezintă o diagramă care ilustrează un proces din stadiul tehnicii de efectuare a explorării de software rău intenționat la acces;

Figura 2 ilustrează schematic un sistem de calculator în conformitate cu aplicații concrete ale invenției prezente;

Figura 3 reprezintă o diagramă care ilustrează un proces de efectuare a explorării de software rău intenționat la acces în conformitate cu o aplicație concretă a invenției prezente;

Figura 4 reprezintă o diagramă de flux care ilustrează un proces în conformitate cu o aplicație concretă a invenției prezente;

Figura 5 ilustrează un tabel de acces la director pentru utilizare în actualizarea și întreținerea directoarelor accesate de către aplicații în conformitate cu aplicații concrete ale invenției prezente;

Figura 6 reprezintă o diagramă de flux care ilustrează un proces de efectuare a explorării de software rău intenționat la acces pentru o aplicație care accesează fișiere în conformitate cu o aplicație concretă a invenției prezente.

Figura 7 reprezintă o diagramă de flux care ilustrează un proces de efectuare a explorării de software rău intenționat la acces pentru o aplicație care accesează fișiere în conformitate cu o altă aplicație concretă a invenției prezente.

Descriere Detaliată

Cu scopul de a depăși cel puțin parțial problemele descrise mai sus, se propune aici să se îmbunătățească performanța unui sistem de calculator prin efectuarea unei explorări de software rău intenționat la acces în șarja sau în paralel de fișiere multiple înainte ca o aplicație să utilizeze unul dintre fișierele multiple. Acest lucru semnifică faptul ca execuția aplicației nu este în întregime blocata în accesări de fișier ulterioare. Așa cum s-a descris anterior, explorarea în șarjă sau în paralel este planificarea simultană a unui grup de fișiere pentru explorare de către un sistem de calculator. De exemplu, planificarea simultană de fire de explorare multiple, câte un fir pentru fiecare fișier din grup, pentru execuție pe sistemul de calculator.

Acest tip de explorare este realizat prin detecția accesărilor de către aplicație la fișiere din cadrul unui director comun, utilizând accesările detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația poate ulterior să vrea să le acceseze, explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor. După explorarea unui grup de fișiere, un grup de fișiere ulterior poate fi identificat și/sau explorat.

Prin efectuarea de explorare în șarjă sau în paralel a unui grup de fișiere pe care aplicația le poate utiliza, șansele ca aplicația să fie blocata sau întreruptă în mod continuu de către o explorare de software rău intenționat este minimizată. Acest lucru apare deoarece aplicația poate accesa și utiliza fișierele explorate dintr-un grup, care acum nu necesita explorare. De fapt, dacă grupul corect de fișiere este identificat pentru fiecare explorare, va exista numai o întârziere a unei explorări de fișier și după aceea execuția aplicației nu ar trebui să fie blocată de către nici o explorare de software rău

intenționat suplimentară atunci când aplicația accesează fișierele explorate. Acest tip de explorare în șarja sau în paralel minimizează întârzierea introdusa de către explorarea de software rău intenționat la acces, astfel optimizând performanță sistemului de calculator.

Figura 2 ilustrează schematic un sistem de calculator 1 și un sistem de calculator la distanță 12 în conformitate cu aplicații concrete ale invenției prezente. Sistemul de calculator 1 poate fi implementat ca o combinație de hardware și software de calculator. Sistemul de calculator 1 cuprinde o memorie 2, o memorie intermediară cu acces rapid (cache) 3, un procesor 4 și un emițător-receptor 5. Memoria 2 stochează toate fișierele necesare pentru sistemul de calculator 1. Fișierele stocate în memoria 2 includ diversele programe/fișiere executabile care sunt implementate de către procesorul 4, precum și oricare fișiere de date 6. Aplicațiile/programele/fișierele executabile stocate în memoria 2, și implementate de către procesorul 4, includ o unitate de detecție 7 și o unitate de explorare de software rău intenționat 8, fiecare dintre acestea putând fi sub-unități ale unei unități anti-virus 9 care pot executa software anti-virus local, precum și sistemul de fișiere 10 și oricare alte programe/aplicații 11. Fișierele de date 6 stocate în memoria 2 pot include fișiere de date de aplicație, tabele de acces la director așa cum sunt definite aici, fișiere de date de definiție de software rău intenționat, fișiere care conțin reguli de analiză euristice, liste albe, liste negre, etc. Memoria cache 3 furnizează o unitate de stocare temporară pentru stocarea de date care trebuie să fie explorate de către unitatea de explorator de software rău intenționat 8. Emițător-receptorul 5 poate fi utilizat pentru a comunica peste un Internet/LAN sau Rețea 13 cu un sistem de calculator la distanță 12. Sistemul de calculator la distanță 12 poate furniza stocare de date și servicii de aplicație la un sistem de calculator 1, de exemplu sistemul de calculator la distanță 12 poate fi un server de aplicație care furnizează aplicații de tipul Software ca un Serviciu (Software as a Service – SaaS) la utilizatorul sistemului de calculator 1.

Sistemul de calculator la distanță 12 este în mod tipic operat de către un furnizor de diverse aplicații care sunt executate pe sistemul la distanță 12 și utilizate la distanță de către utilizatorul sistemului de calculator 1. Sistemul de calculator la distanță 12

poate fi implementat ca o combinație de hardware și software de calculator cum este pentru sistemul de calculator 1. Sistemul de calculator la distanță 12 cuprinde o memorie 14, un procesor 15, și un emițător-receptor 16. În privința sistemului de calculator 1, memoria 14 poate stoca fișiere care includ diverse aplicații/programe/fișiere executabile care sunt implementate de către procesorul 15, precum și oricare fișiere de date 16. Aplicațiile/programele/fișierele executabile stocate în memoria 14, și implementate de către procesorul 15 de asemenea includ o unitate de detecție 18 și o unitate de explorator de software rău intenționat 19, fiecare dintre acestea putând fi sub-unități ale unei unități anti-virus 20 care executa software anti-virus local pe sistemul la distanță 12. Emițător-receptorul 16 este utilizat pentru a comunica cu sistemul de calculator 1 peste rețeaua 13.

În operațiune utilizatorul sistemului de calculator 1 poate executa aplicații local, sau poate executa aplicații pe sistemul de calculator la distanță 12. Unitatea de explorator pentru software rău intenționat 8 a sistemului de calculator 1 poate fi utilizată pentru a explora fișiere locale pentru software rău intenționat din memoria 2 accesate de către aplicații locale. Unitatea de explorator de software rău intenționat 19 a sistemului la distanță 12 poate fi utilizată pentru a explora fișiere pentru software rău intenționat în memoria 14 accesata de către aplicațiile sistemului la distanță 12. Metodele de explorare a fișierelor din oricare dintre aceste sisteme pot fi bazate pe acelea în conformitate cu invenția prezentă. Trebuie să fie apreciat faptul că aplicațiile concrete ale invenției, așa cum sunt descrise aici, pot fi implementate în sisteme de calcul independente sau legate la rețea prin intermediul sistemelor de calcul distribuite unde fișierele și aplicațiile sunt stocate și executate la distanță.

În particular, sistemele de calculator 1 sau 12 sunt configurate pentru a explora fișierele pentru software rău intenționat în timpul execuției unei aplicații sau a aplicațiilor care executa pe oricare dintre procesoarele 4 sau 15, în mod corespunzător. Sistemele de calculator 1 sau 12 includ unitățile de detecție 7 sau 18, în mod corespunzător, pentru detecția accesărilor de către aplicație la fișierele din cadrul unui director comun, și utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere

din cadrul directorului comun menționat pe care aplicația poate să dorească să le acceseze ulterior, și instruirea unităților de explorare 8 sau 19, în mod corespunzător, pentru explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor. Așa cum este ilustrat sistemele de calculator 1 sau 12 deja includ unitățile de explorare 8 sau 19 pentru explorarea unuia sau mai multor grupuri de fișiere menționate ca răspuns la instruirea unităților de detecție 7 sau 18, în mod corespunzător. Trebuie să fie apreciat faptul că deși explorarea unităților 8 sau 19 este implementată în cadrul unităților anti-virus 9 și 20, în mod corespunzător, unitățile de explorare 8 sau 9 ar putea fi de asemenea implementate pe alte sisteme de calculator/servere astfel încât unitatea de detecție 7 sau 18 trimite instrucțiuni peste rețeaua 13 pentru a avea grupurile de fișiere, care sunt unul sau mai multe, explorate.

Trebuie să fie apreciat faptul că aplicațiile concrete ale invenției pot fi utilizate într-un sistem de calcul de Nor sau de calcul distribuit. De exemplu, o aplicație poate executa pe sistemul de calculator la distanță 12 și accesează fișiere de la un centru de date la distanță (nu este prezentat) unde detecția accesărilor de fișier este efectuată la centrul de date dar explorarea de software rău intenționat este efectuată la sistemul de calculator la distanță 12. Sistemul de calculator la distanță 12 poate efectua explorare de „Nor", care este un exemplu de furnizare a capacității de explorare pentru software rău intenționat peste o rețea sau un sistem de calculator distribuit. Pentru a minimiza suprasarcina implicată în explorarea fișierelor peste o rețea, adică minimizarea lățimii de bandă, explorarea poate fi limitată la verificarea meta-datelor de fișier stocate în centrul de date la distanță (serverul la distanță sau partea de susținere (backend)). Meta-datele ar putea fi create pentru fiecare fișier de la un șir de octeti de comprimare (hash) (de exemplu sha1) calculat de la datele fișierului sau de la porțiuni specifice ale datelor fișierului. Numai meta-datele sunt încărcate și explorate de către sistemul de calculator la distanță 12 atunci când acesta detectează accesări generate de către o aplicație de utilizator la fișiere. Sistemul de calculator gazdă al utilizatorului 1 ar putea interoga sistemul de calculator la distanță 12 în legătură cu datele fișierului explorat și

recepționează starea pe baza unei explorări de verificare limitate (curățire, nume fișier infectat și software rău intenționat).

Aplicațiile concrete ale invenției permit explorarea paralelă (de exemplu explorare cu fire multiple) pe un sistem de calcul 1 sau sistem de calcul la distanță 14 pentru solicitări de explorare cum ar fi solicitări de explorare la acces de deschidere de fișier numai pentru citire. Metodele descrise aici sunt bazate pe analizarea comportamentului uneia sau mai multor aplicații pentru a găsi dependențe atunci când o aplicație generează acces secvențial pentru fișiere multiple dintr-un director de lucru curent al aplicației sau un director comun. Termenul director comun se referă la aceeași locație logică din memorie (de exemplu, dispozitiv de disc) unde unul sau mai multe fișiere sunt stocate. Performanța este optimizată datorita faptului că aplicațiile accesează în mod comun mai multe fișiere din același dosar sau director. Dacă software-ul anti-virus recunoaște acest tip de model de comportament de aplicație atunci acesta poate efectua explorare în avans asupra unui grup de fișiere pe care aplicația poate ulterior dori să le acceseze sau să le utilizeze. Software-ul anti-virus apoi efectuează explorare la acces pe grupuri de fișiere multiple pentru software rău intenționat.

Figura 3 ilustrează procesul de efectuare de explorare de software rău intenționat la acces în șarjă sau în paralel în conformitate cu o aplicație concretă a invenției prezente. Software-ul anti-virus grupează fișiere multiple împreună în dependență de comportamentul aplicațiilor care accesează fișierele și execută explorare de căutare în avans pe grupuri de fișiere multiple. Rezultatele explorărilor sunt memorate în cache și dacă aplicația accesează fișierul explorat prin căutare în avans aceasta recepționează un răspuns de la memoria cache despre faptul că fișierul a fost explorat și poate continua să utilizeze fișierul.

În practică, explorarea de fișier normală este implementată în modul de utilizator și software-ul anti-virus interceptează accesările de fișier de nivel redus de către aplicație și trimite o solicitare de explorare la modul de utilizator. Aceasta este o operațiune scumpă și necesita comutație de context (nucleu la mod de utilizator și din

nou înapoi). Trebuie să fie apreciat faptul ca metodele de explorare, așa cum sunt descrise aici, reduc apelurile înapoi de la aplicație la software-ul anti-virus, care îmbunătățesc în mod considerabil performanța. De exemplu, software-ul anti-virus are un driver de filtru de nucleu care interceptează aplicații care încearcă să acceseze sau să deschidă fișiere. Driver-ul de filtru de nucleu trimite o solicitare la modul de utilizator pentru a efectua o sarcină de explorare pe fișierul pe care o aplicație încearcă să-l acceseze. Serviciul de explorare care executa în modul de utilizator efectuează o explorare de software rău intenționat reală pe fișier și notifică rezultatele și starea explorării înapoi la driver-ul de filtru de nucleu. Pe baza acestor rezultate driver-ul de filtru de nucleu permite sau respinge aplicației accesul la fișier.

Cu referință la figura 3, atunci când aplicația deschide fișierul denumit file1, software-ul anti-virus interceptează solicitarea aplicației de a deschide fișierul 1. Software-ul anti-virus, care a determinat faptul că o explorare în șarja sau în paralel este necesară de la comportamentul aplicației, efectuează o explorare de șarjă sau paralelă pe un grup de fișiere, care poate include fișierul solicitat (de exemplu, file1, file2, și file3). Odată ce file1, file2, și file3 au fost explorate rezultatele sunt memorate în cache și aplicația poate continua să deschidă și să utilizeze file1 în mod normal. Deoarece file2 și file3 au fost de asemenea explorate, atunci când aplicația deschide aceste fișiere aceasta recepționează un răspuns de la memoria cache care permite aplicației să deschidă și să utilizeze imediat file2 și file3 (în dependență de răspuns). În acest exemplu, explorarea în șarja sau în paralel a grupului de fișiere permite aplicației să execute fără o întrerupere suplimentară.

Deși explorarea în șarjă sau paralelă a unui grup de fișiere poate îmbunătăți în mod substanțial performanța generala a unei aplicații sau a aplicațiilor care executa pe un sistem de calcul, performanță este îmbunătățita în mod substanțial dacă grupul de fișiere explorate include numai acele fișiere care sunt necesare pentru aplicație/aplicații. Explorarea fișierelor care nu sunt utilizate de către o aplicație poate impacta performanța cu excepția cazului în care acel fișier va fi utilizat de către o altă aplicație. De exemplu, dacă software-ul anti-virus explorează în avans prea multe fișiere, care nu

vor fi accesate de către oricare aplicație, atunci acesta numai reduce performanță generală deoarece resursele calculatorului sunt utilizate pentru explorarea fișierelor ne-necesare. Următoarele aplicații concrete ale invenției prezente descriu metode pentru minimizarea explorărilor de fișier ne-necesare, ceea ce maximizează performanță aplicației sau a aplicațiilor și a sistemului de calcul.

Figura 4 reprezintă o diagramă de flux care ilustrează suplimentar procesul de explorare pentru software rău intenționat în timpul execuției uneia sau mai multor aplicații pe un sistem de calculator în conformitate cu o aplicație concretă a invenției prezente. Procesele efectuate de către o unitate de explorare sau un software anti-virus pentru fiecare aplicație care accesează fișiere din cadrul unui director comun sunt schițate după cum urmează:

A1. Detecția accesărilor de către aplicație la fișierele din cadrul unui director comun.

A2. Utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația poate dori ulterior să le acceseze.

A3. Explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor.

Cu privire la pasul A1, detecția accesărilor de către aplicație la fișierele din cadrul directorului comun poate include recepția unei solicitări de explorare pentru explorarea unui fișier accesat de către aplicație (fișierul curent accesat) din cadrul directorului comun. Detecția accesului la fișier de către aplicație poate de asemenea include intercepția accesului la fișier realizate de către aplicație și generarea solicitării de explorare și trimiterea solicitării de explorare, atunci când explorarea este solicitată, la software-ul anti-virus pentru explorare.

Cu privire la pasul A2, utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere poate include pasul de selecție a grupului sau grupurilor de fișiere pe baza tipurilor de fișier a fișierelor accesate de către aplicație. Acest lucru poate implica selecția de fișiere care pun în corespondență tipurile de fișier ale fișierelor accesate de către aplicație cu tipurile de fișier sau fișierele din cadrul directorului comun. Suplimentar, fișierele din cadrul grupului sau grupurilor de fișiere pot fi selectate de la fișierele din cadrul directorului comun care necesită explorare. Fișierul curent detectat ca fiind accesat de către aplicație poate fi adăugat la grupul de fișiere pentru explorare dacă fișierul curent necesită explorare.

Cu scopul de a utiliza accesările detectate și pentru a declanșa explorarea grupului sau grupurilor de fișiere, pasul A2 poate include determinarea numărului de accesări detectate din cadrul directorului comun și utilizarea rezultatelor pentru a declanșa pasul de explorare a grupurilor, care sunt unul sau mai multe. Declanșarea explorării poate apare atunci când numărul de accesări detectate atinge un prag, *N*. Acest prag ar putea fi un prag predeterminat, sau un prag dinamic determinat de către software-ul anti-virus și comportamentul observat al acestuia la una sau mai multe aplicații care accesează fișierele din cadrul directorului comun. Fișierul curent detectat pentru a fi accesat de către una sau mai multe aplicații poate fi adăugat la grupul de fișiere. Acest lucru poate apare înainte sau atunci când pasul de explorare este declanșat. Fișierul curent accesat poate corespunde la fișierul care corespunde la solicitarea de explorare recepționată. Fișierul curent este apoi adăugat la grupul de fișiere pentru explorare. Grupul de fișiere este explorat pe baza solicitării de explorare recepționate de către anti-virus pentru fișierul curent. Cu scopul de a evita explorarea nenecesară atunci când aplicațiile accesează un director nefrecvent, pasul de detecție a numărului de accesări poate include resetarea numărului de accesări detectate atunci când o primă perioadă de timp a trecut și pasul de explorare nu a fost declanșat.

Așa cum s-a explicat mai jos, utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere poate include întreținerea unei liste de tipuri de

fișier ale fișierelor detectate accesate și pasul de identificare a unuia sau mai multor grupuri de fișiere include pasul de selecție a fișierelor pe baza listei de tipuri de fișier. Selectarea fișierelor include suplimentar punerea în corespondență a listei de tipuri de fișiere ale fișierelor accesate de către aplicație cu tipurile de fișier ale fișierelor din cadrul unui director comun. Software-ul anti-virus poate întreține o listă pentru fiecare director comun care are fișiere accesate în mod frecvent de către una sau mai multe aplicații.

În privința pasului A3, utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere poate include urmărirea numărului de accesări detectate și de la rezultate declanșarea pasul A3. Declanșarea pasului A3 ar putea apărea atunci când numărul de accesări detectate atinge un prag predeterminat sau un prag de explorare. Identificarea unuia sau mai multor grupuri de fișiere pentru explorare poate include selecția fișierelor din cadrul directorului comun pe baza tipurilor de fișier care au fost accesate anterior sau sunt accesate de către aplicație. Ca alternativă, o selecție a grupurilor poate fi determinată de la o listă stocată a tipurilor sau numelor de fișiere accesate de către de către diverse aplicații din cadrul directorului comun. Suplimentar, pasul A3 poate include terminarea exploatării după ce o perioadă de timp predeterminată a trecut, de exemplu dacă directorul a fost accesat în mod frecvent dar nu a fost accesat pentru o perioada de timp care justifică terminarea explorării directorului, atunci explorarea unuia sau mai multor grupuri de fișiere ar putea fi terminată pentru a evita procesarea nenecesară. Acest lucru poate apare atunci când o a doua perioadă de timp a trecut după ce pasul de explorare a fost declanșat.

Urmărirea numărului de accesări detectate (sau numărul de atingeri) la directorul comun ajută să se determine dacă aplicațiile accesează în mod activ directorul. Dacă directorul are un „număr de atingeri" suficient de înalt datorită faptului că este accesat peste o perioadă scurtă de timp, atunci, pentru accesările de fișier ulterioare din director, software-ul anti-virus poate explora în mod simultan o șarjă de fișiere selectate de la tipurile de fișier de explorare prevalente sau de la tipul de fișier accesat și fișierului curent accesat. Așa cum s-a menționat anterior, explorarea în mod simultan poate fi realizată prin planificarea în mod simultan de fire de explorare multiple pentru

explorarea fișierelor, adică explorarea în paralel sau în șarjă. Explorarea este declanșată odată ce numărul de accesări detectate atinge un prag.

Explorarea trebuie să fie efectuată pe un grup de fișiere dacă se detectează faptul că fișierul curent pe care o aplicație îl detectează este un fișier neexplorat. În acest caz, accesul de fișier este detectat sau interceptat de către un driver de filtru nucleu, care generează o solicitare de explorare care este recepționată de către software-ul anti-virus pentru explorarea fișierului accesat curent. În locul explorării numai a fișierului ne-explorat, anti-virusul nu numai că explorează fișierul neexplorat care a fost accesat, dar de asemenea încarcă un grup sau grupuri de fișiere pentru explorare. Software-ul anti-virus execută explorarea solicitării de explorare curente (solicitarea de explorare pentru fișierul curent accesat) și în mod simultan planifică (sau execută) explorarea de mai multe „solicitări de explorare purtate în spate" a fișierelor de la o listă încărcată. Lista încărcată este o listă de fișiere generate de către anti-virus care poate fi accesată de la director – aceasta poate include tipuri de fișier accesate în mod prevalent. Anti-virusul încarcă o selecție de fișiere de la director pe baza listei încărcate.

De exemplu, dacă un director (sau un dosar) are fișierele A,B, C, D, E, atunci la momentul de timp la care fișierele A și B au fost explorate se poate considera faptul că acest director a fost accesat în mod frecvent. Dacă C, D, și E au fost puse pe lista încărcată, atunci când explorarea este declanșată de către accesările frecvente, anti-virusul încarcă fișierele C, D, E (A. B sunt omise deoarece acestea sunt deja explorate). Dacă se detectează faptul că fișierul C este accesat de către aplicație, atunci o solicitare de explorare pentru fișierul C va fie recepționată de către anti-virus pentru explorare, care explorează fișierul C împreună cu explorarea fișierelor D și E. Aceasta semnifică faptul că atunci când fișierele D și E sunt ulterior accesate de către o aplicație, atunci solicitările de explorare pentru aceste fișiere nu vor fi generate de către driver-ul de filtru deoarece aceste fișiere au fost deja explorate.

Grupul sau grupurile de fișiere sunt fișiere selectate de la directorul pe care aplicație poate ulterior să vrea să le acceseze. Explorarea grupului sau grupurilor „duce

în spate" explorarea fișierului accesat curent, adică, duce în spate solicitarea de explorare a fișierului curent. Acest lucru împiedica solicitări de explorare viitoare care sunt generate sau realizate pentru fișierele grupului.

Chiar dacă unele dintre fișierele selectate pentru explorare „dusă în spate" nu sunt accesate de către aplicație, pierderea de performanță într-o singură șarjă „dusă în spate" este neglijabilă datorită explorării în șarjă sau în paralel. Atunci când o aplicație efectuează procesare lungă (de exemplu copierea unui întreg dosar de date) acest tip de explorare cu căutare în avans crește considerabil performanță generală. Software-ul anti-virus estimează multitudinea de fișiere care trebuie să fie accesate din director prin selecția fișierelor celor mai comune pe care aplicațiile le-au accesat din director peste o perioada de timp particulară. Acest lucru poate fi efectuat prin întreținerea unui tabel la momentul execuției de accesări de director, care depinde de comportamentul diverselor aplicații care sunt executate.

Figura 5 reprezintă un tabel de acces la director care ilustrează actualizarea și întreținerea accesărilor detectate de către aplicații la fișiere din cadrul unuia sau mai multor directoare în conformitate cu aplicații concrete ale invenției prezente. Tabelul de acces la director poate fi implementat ca un tabel de căutare la momentul execuției stocat în memorie. Tabelul este întreținut de către software-ul anti-virus pentru utilizare în determinarea numărului de ori de care fișierele din director sunt accesate.

Software-ul anti-virus întreține tabelul de acces la director la momentul execuției (sau tabelul de acces la director), care urmărește accesul fișierelor în interiorul directoarelor de către aplicații. În această aplicație concreta, tabelul de acces la director are următoarele câmpuri:

- Drumul de director, care menține numele sau locația logică a directorului în care unul sau mai multe fișiere sunt accesate;
- Lista de extensii accesate, care conține o listă a extensiilor de fișier a fișierelor care au fost accesate și explorate din director;
- Numărul de atingeri, care prezintă numărul de accesări la fișier din director; și

- Starea elementului, care definește ciclul de viață al elementului directorului

În această aplicație concretă, câmpul de Stare de Element are 3 stări logice *Remarcat*, *Colectat*, și *Procesat*. Starea *Remarcat* (adică o stare de pre-explorare) indică faptul că fișierul a fost accesat în director dar că numărul de atingeri ale directorului nu este încă suficient pentru a garanta explorarea paralelă sau în șarjă. Odată ce numărul de atingeri ajunge la un prag, Starea de Element a directorului este schimbată la starea *Colectat* (adică o stare de explorare). Starea *Colectat* semnifică faptul că directorul a fost sau este accesat în mod activ de către o aplicație, ceea ce garantează explorarea paralelă sau în șarjă. Software-ul anti-virus pre-încarcă grupuri de fișiere având extensii de fișier listate în *Lista de Extensii Accesate*, sau extensii de fișier ale fișierului curent care este accesat pentru explorare paralelă sau în șarjă. Starea *Procesat* semnifică faptul că explorarea cu căutare în avans a fost deja efectuată pentru director și fișierele ar trebui să fie explorate în mod normal.

Fiecare stare are o perioadă de valabilitate, după expirare elementul de director este eliminat din tabelul de acces, de exemplu dacă nici un fișier nu este accesat dintr-un director pentru o perioadă de timp, atunci elementul este considerat ca fiind expirat. Starea *Remarcat* are o perioadă de valabilitate scurtă și servește pur și simplu pentru a recunoaște directoarele care pot fi accesate în mod frecvent. Stările *Colectat* și *Procesat* au perioade mai lungi de valabilitate datorită frecvenței accesărilor și pentru a evita re-explorarea nenecesară a fișierelor accesate din director. Trebuie să fie apreciat faptul că aceste perioade pot fi variate de către software-ul anti-virus pe baza oricărei scale de timp.

Este de apreciat faptul că câmpul de Stare de Element este utilizat pentru a exclude reîncărcarea și explorarea unui director dacă acesta a fost procesat numai recent (de exemplu, cu 10 minute în urmă). Alte implementări ale tabelului de acces la director pot exclude acest câmp și se bazează pe temporizatoare sau alte mijloace pentru a împiedica un director de la a fi explorat într-un mod prea regulat după ce acesta a fost procesat.

Figura 6 reprezintă o diagramă de flux care ilustrează suplimentar procesul de utilizare a tabelului din figura 5 în efectuarea explorării de software rău intenționat la acces în paralel sau în șarjă în conformitate cu o aplicație concretă a invenției prezente. Pașii metodei sunt efectuați de către software-ul anti-virus după cum urmează:

B1. Pentru fiecare fișier interceptat pentru explorarea de software rău intenționat, de exemplu o solicitare de explorare este generată pentru o deschidere de fișier, se continuă la pasul B2 pentru a verifica tabelul de acces.

B2. Verifică dacă directorul fișierului este în tabelul de acces, dacă directorul nu este în tabelul de acces, atunci se continuă la pasul B3 pentru a crea un element de director, altfel se continuă la pasul B4.

B3. Creează un element de tabel de acces pentru directorul de fișier, și inițializează Starea de Element a directorului la *Remarcat*, Numărul de Atingeri = 0, extensia de fișier a fișierului este adăugată la Lista de Extensii de Fișier (sau lista de tipuri de fișier explorată), continuă să efectueze explorare de software rău intenționat normală a fișierului accesat.

B4. Verifică dacă Starea Elementului directorului este în starea *Remarcat*, dacă Starea Elementului este *Remarcat* atunci se continuă la pasul B5, altfel se continuă la pasul B8.

B5. Incrementează Numărul de Atingeri care reprezintă numărul de accesări de fișier din director prin diverse aplicații și adaugă extensia de fișier a fișierului la Lista de Extensii Accesate.

B6. Verifică dacă Numărul de Atingeri (HC) ajunge la o valoare de prag *N* (de exemplu *HC* >= *N*, unde *N*=5). Dacă Numărul de Atingeri ajunge la valoarea de prag,

atunci se continuă la pasul B7, altfel explorarea de software rău intenționat normală este efectuată pe fișierul accesat.

B7. Starea de Element a directorului este modificată la starea *Colectat* și procesul continuă la pasul B8, unde software-ul anti-virus încarcă un grup de fișiere care include fișierul accesat pentru explorarea în paralel sau în șarja de la director.

B8. Verifică dacă Starea de Element a directorului este în starea *Colectat*, dacă Starea Elementului este *Colectat* atunci continuă la pasul B9, altfel continuă la pasul B10.

B9. Efectuează o explorare de software rău intenționat în paralel (sau în șarjă) pe un grup sau o selecție de fișiere neexplorate care include fișierul curent din director.

Următoarele reguli pot fi utilizate pentru selecția unui grup de fișiere pentru explorarea în șarja sau în paralel:

- Selectează fișiere cu extensii sau tipuri de fișier care corespund la fișierul accesat în mod curent; sau
- Selectează fișiere cu extensii sau tipuri de fișier listate în Lista de Extensii Accesate.

B10. Verifica dacă mai multe grupuri de fișiere există în director. Fișierele pot fi selectate din lista încărcată. Dacă există mai multe grupuri de fișiere, metoda continuă la pasul B11, altfel metoda continuă la pasul B12.

B11. Un alt grup de fișiere neexplorate este selectat din lista încărcată, și o explorare de software rău intenționat în șarjă sau în paralel este efectuată, metoda continua la pasul B10. Deși software-ul anti-virus este intenționat pentru a evita blocarea execuției unei aplicații, acest lucru poate fi realizat dacă suportul de nucleu multiplu este capabil de sarcini multiple între aplicație și software-ul anti-virus. Aceasta este

explorarea în șarjă sau în paralel a fișierelor neexplorate suplimentare din listă care ar putea fi efectuata în fundal astfel încât aplicația să poată continua.

B12. Deoarece nu mai există fișiere încărcate sau fișiere neexplorate având extensii de fișier listate în Lista de Extensii de Acces în director, atunci Starea de Element a directorului este modificată la starea Procesat. Dacă un director este găsit în starea Procesat, procesul efectuează o explorare de software rău intenționat normală a fișierului dacă este necesar.

Rezultatele explorărilor de software rău intenționat sunt adăugate în memoria cache de explorare și sunt raportate la aplicație atunci când aceasta accesează un fișier explorat din director, permițând aplicației să utilizeze imediat fișierul accesat.

Figura 7 reprezintă o diagramă de flux alternativă care ilustrează explorarea de software rău intenționat la acces în șarjă sau în paralel în conformitate cu o aplicație concretă a invenției prezente. Pașii de metodă de la B1 la B12 care sunt efectuați de către software-ul anti-virus sunt similari cu cei ai figurii 6, cu excepția pașilor B10 și B11 (B11 a fost eliminat). Pasul B10 este descris după cum urmează:

B10. Verifică dacă mai multe grupuri de fișiere există în director. Fișierele pot fi selectate de la lista încărcată. Dacă mai multe grupuri de fișiere există, metoda continuă la explorarea de software rău intenționat normal până când un fișier suplimentar este accesat de către aplicația care solicită explorare, unde metoda începe din nou la pasul B1.

Motivul pentru ne-continuarea de a efectua o explorare în paralel suplimentară a altor grupuri de fișiere este acela că aplicația are nevoie să acceseze numai un număr limitat de fișiere din director, acest proces împiedică software-ul anti-virus de la efectuarea unei explorări în șarjă sau în paralel în fundal pe toate fișierele listate în Lista de Extensii de Acces până când este absolut necesar atunci când un alt fișier este

accesat de către o aplicație. Acest lucru de asemenea minimizează numărul de întreruperi de explorare de software rău intenționat în timpul execuției unei aplicații.

Exemplul următor ilustrează modul în care metoda menționată mai sus poate opera atunci când se copiază o multitudine de fișiere de la un director comun. Sunt făcute următoarele presupuneri:

a) Directorul comun are o colecție de fișiere *.exe și *.dll;
b) Tabelul de acces este întreținut de către programul anti-virus;
c) Tabelul de acces deja are un element de director în legătura cu directorul comun;
d) Un număr de atingeri care reprezintă numărul de accesări și o listă de extensii de fișier accesate din directorul comun sunt întreținute.

Fluxul de logică este după cum urmează:

1. Primele câteva fișiere „exe" accesate sunt explorate în mod normal până când directorul colectează un număr suficient de atingeri, adică numărul de atingeri ajunge la un prag;
2. Cât de curând numărul de atingeri ajunge la un prag, software-ul anti-virus încarcă fișierele din director;
3. Oricare solicitare de explorare următoare de fișiere „exe" din director declanșează o explorare „de ducere în spate" a altor fișiere „exe" (un grup de fișiere) din director;
4. După ce copierea este terminată elementul de director expiră după o perioadă de timp.

Mai în detaliu, atunci când operațiunea de copiere, copy *<de la directorul comun>*.exe <la un alt director>* este efectuată, comanda de copiere (aplicația) va accesa fișierele „exe" în mod secvențial pentru a citi și a copia date în celălalt director. Atunci când primul fișier „exe" este accesat de la directorul comun, o solicitate de explorare va fi generata pentru software-ul anti-virus. Dacă directorul comun nu are un element de director în tabelul de acces, software-ul anti-virus va crea și va inițializa un

element de director pentru directorul comun, numărul de atingeri al elementului de director care reprezintă numărul de accesări de fișier este inițializat și tipul de fișier, în acest caz „exe", este adăugat la o listă de extensie în legătură cu elementul de director. Altfel, numărul de atingeri al elementului de director este incrementat și tipul de fișier „exe" este adăugat la lista de extensie dacă acesta nu este deja în lista de extensie.

Primul fișier „exe" accesat este apoi explorat în mod normal pentru software rău intenționat și utilizat de către comanda copy. Fișiere „exe" ulterioare sunt accesate, solicitări de explorare sunt realizate și sunt explorate normal de către software-ul anti-virus și numărul de atingeri pentru elementul directorului comun este incrementat pe fiecare acces până când elementul de director în legătură cu directorul comun colectează un număr suficient de atingeri. Cât de curând numărul de atingeri ajunge la un prag, software-ul anti-virus începe să încarce sau determină unul sau mai multe grupuri de fișiere „exe" neexplorate de la directorul comun. Fiecare solicitare de explorare următoare a unui fișier „exe" neexplorat declanșează anti-virusul pentru a efectua explorarea în paralel (adică în mod substanțial explorare simultană) a fișierului „exe" neexplorat și a unuia din grupurile de fișiere neexplorate de la directorul comun. Explorarea continuă până când fișierele „exe" relevante din directorul comun au fost procesate sau comanda copy se termină. După ce comanda copy se termină, elementul de director din tabelul de acces va expira într-un cadru de timp predeterminat și este eliminat din tabelul de acces la expirare.

Sistemele de calcul așa cum sunt descrise aici fiecare poate efectua explorare în șarja sau în paralel a unui grup de fișiere selectate dintr-o multitudine de fișiere accesate de la un director comun pentru software rău intenționat. Procesoarele unor astfel de sisteme sunt configurate pentru a executa instrucțiuni de program de calculator pe baza metodelor descrise aici, astfel de instrucțiuni fiind conținute într-un mediu care poate fi citit de calculator, cum ar fi o memorie. Instrucțiunile programului de calculator pot fi citite în memorie de la un alt mediu care poate fi citit de calculator sau de la un alt dispozitiv prin intermediul unei interfețe de comunicație. Instrucțiunile conținute în memorie fac ca procesorul sistemului de calcul să efectueze procedurile sau

metodele așa cum este descris aici. Cu toate acestea, ca alternativă, circuite cablate hardware pot fi utilizate în locul sau în combinație cu instrucțiunile de program de calculator pentru a implementa procese consistente cu invenția prezentă. Astfel, invenția prezentă nu este limitată la nici o combinație specifică de circuite hardware și/sau de software.

În particular, un program de calculator care include mijloace de cod de program de calculator adaptate pentru a efectua pașii de detecție a accesărilor de către aplicație la fișierele din cadrul unui director comun, utilizând accesările detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația poate dori ulterior să le acceseze, și instruind explorarea grupurilor de fișiere menționate, care sunt unul sau mai multor, pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor. Programul de calculator poate suplimentar include mijloace de cod de program de calculator adaptate suplimentar pentru a efectua explorarea unuia sau mai multor grupuri de fișiere menționate. Programul de calculator poate fii încorporat pe un mediu care poate fi citit de calculator.

Suplimentar, metodele descrise mai sus pot exploata capacitățile de multi-procesor, sarcini multiple, fire de execuție multiple și hiper fire de execuție (hyper-threading) ale sistemelor de calculator moderne (așa cum este descris aici și de asemenea în documentul Tehnologia Hyper-Threading de la Intel®, Ghidul Utilizatorului Tehnic (Inter® Hyper-Threading Technology, Technical User's Guide), Ianuarie 2003) pentru a îmbunătăți suplimentar performanța unui sistem de calculator atunci când se implementează explorare de software rău intenționat la acces la deschidere de fișier numai pentru citire, prin permiterea ca explorarea unuia sau mai multor grupuri de fișiere să fie paralelizată.

Se va aprecia de către persoana cu calificare în domeniu faptul că diverse modificări pot fi realizate la aplicațiile concrete descrise mai sus fără îndepărtarea de la scopul invenției prezente.

Revendicări

1. Metodă de explorare pentru software rău intenționat în timpul execuției unei aplicații pe un sistem de calculator, metoda cuprinzând:

detectarea accesărilor de către aplicație a fișierelor din cadrul unui director comun;

utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun pe care aplicația poate ulterior dori să le acceseze; și

explorarea acelui unul sau mai multe grupuri de fișiere, pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor.

2. Metodă în conformitate cu revendicarea 1, în care pasul de utilizare a accesărilor detectate pentru a identifica grupurile de fișiere, care sunt unul sau mai multe, include pasul de selecție a grupului sau grupurilor de fișiere pe baza tipurilor de fișier a fișierelor accesate de către aplicație.

3. Metodă în conformitate cu revendicarea 2, în care pasul de selecție a fișierelor include suplimentar punerea în corespondență a tipurilor de fișiere accesate de către aplicație cu tipurile de fișier ale fișierelor din cadrul directorului comun.

4. Metodă în conformitate cu oricare dintre revendicările de la 1 la 3, în care fișierele din cadrul grupului sau grupurilor de fișiere sunt fișiere care necesită explorare.

5. Metodă în conformitate cu oricare dintre revendicările de la 1 la 4, în care pasul de identificare a unuia sau mai multor grupuri de fișiere include pasul de adăugare a fișierului curent detectat pentru a fi accesat de către aplicație la grupul de fișiere pentru explorare atunci când fișierul curent necesită explorare.

6. Metodă în conformitate cu oricare dintre revendicările de la 1 la 5, în care pasul de utilizare a accesărilor detectate include pasul de determinare a numărului de

accesări detectate în cadrul directorului comun și utilizarea rezultatelor pentru a declanșa pasul de explorare a aceului unul sau mai multe grupuri.

7. Metodă în conformitate cu revendicarea 6, în care pasul de declanșare a pasului de explorare apare atunci când numărul de accesări detectate atinge un prag predeterminat.

8. Metodă în conformitate cu revendicările 6 sau 7, în care utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere include pasul de adăugare a fișierului curent detectat ca fiind accesat de către aplicație la un grup de fișiere atunci când pasul de explorare este declanșat.

9. Metodă în conformitate cu oricare dintre revendicările de la 6 la 8, în care determinarea numărului de accesări detectate include pasul de resetare a numărului de accesări detectate atunci când o primă perioada de timp a trecut și pasul de explorare nu a fost declanșat.

10. Metodă în conformitate cu revendicările de la 6 la 9, în care pasul de explorare a unuia sau mai multor grupuri de fișiere include pasul de terminare a explorării grupului sau grupurilor atunci când o a doua perioadă de timp a trecut după ce pasul de explorare a fost declanșat.

11. Metodă în conformitate cu oricare dintre revendicările de la 1 la 10, în care pasul de utilizare a accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere include pasul de întreținere a unei liste de tipuri de fișiere a fișierelor detectate accesate și pasul de identificare a unuia sau mai multor grupuri de fișiere include pasul de selectare a fișierelor pe baza listei de tipuri de fișiere.

12. Metodă în conformitate cu revendicarea 11, în care pasul de selecție a fișierelor include suplimentar punerea în corespondență a listei de tipuri de fișiere a

fișierelor accesate de către aplicație cu tipurile de fișiere ale fișierelor din cadrul directorului comun.

13. Metodă în conformitate cu revendicările 11 sau 12, în care fișierele din cadrul grupului sau grupurilor de fișiere sunt fișiere din cadrul directorului comun care necesită explorare.

14. Metodă în conformitate cu oricare dintre revendicările de la 11 la 13, în care pasul de identificare a unuia sau mai multor grupuri de fișiere include pasul de adăugare a fișierului curent detectat pentru a fi accesat de către aplicație la un grup de fișiere pentru explorare.

15. Metodă în conformitate cu oricare dintre revendicările de la 1 la 14, în care pasul de detecție de accesări de către aplicație la fișiere din cadrul directorului comun include recepția unei solicitări de explorare pentru explorarea unui fișier accesat de către aplicație din cadrul directorului comun.

16. Metodă în conformitate cu revendicarea 15, în care pasul de identificare a unuia sau mai multor grupuri de fișiere include pasul de adăugare a fișierului care corespunde la solicitarea de explorare la grupul de fișiere pentru explorare.

17. Program de calculator pentru explorarea software-ului rău intenționat în timpul execuției unei aplicații pe un sistem de calculator care cuprinde mijloace de cod de program de calculator adaptate pentru a efectua pașii următori:

detecția accesărilor de către aplicație la fișiere din cadrul directorului comun;

utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere în cadrul directorului comun menționat pe care aplicația poate ulterior să dorească să le acceseze; și

instruirea explorării acelui unul sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișiere ale grupului sau grupurilor.

18. Program de calculator în conformitate cu revendicarea 17 care cuprinde suplimentar mijloace de cod de program de calculator adaptate pentru a efectua explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat ca răspuns la pasul de instruire.

19. Program de calculator în conformitate cu revendicările 17 sau 18 încorporat pe un mediu care poate fi citit de calculator.

20. Sistem de calculator configurat pentru a explora fișiere pentru software rău intenționat în timpul execuției unei aplicații pe un procesor, sistemul de calculator cuprinzând:

o unitate de detecție pentru detecția accesărilor de către aplicație a fișierelor din cadrul unui director comun, și utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fișiere din cadrul directorului comun menționat pe care aplicația ar putea dori ulterior să le acceseze, și instruirea unei unități de explorare pentru explorarea unuia sau mai multor grupuri de fișiere menționate pentru software rău intenționat înainte ca aplicația să încerce să acceseze fișierele grupului sau grupurilor.

21. Sistem de calculator în conformitate cu revendicarea 20, care cuprinde suplimentar o unitate de explorare pentru explorarea unuia sau mai multor grupuri de fișiere menționate ca răspuns la instruirea de către unitatea de detecție.

22. Produs program de calculator care cuprinde cod de instrucțiune, care atunci când este executat pe un procesor, efectuează metoda în conformitate cu oricare dintre revendicările de la 1 la 16

a-2013 00848--
29 -03- 2013

M2

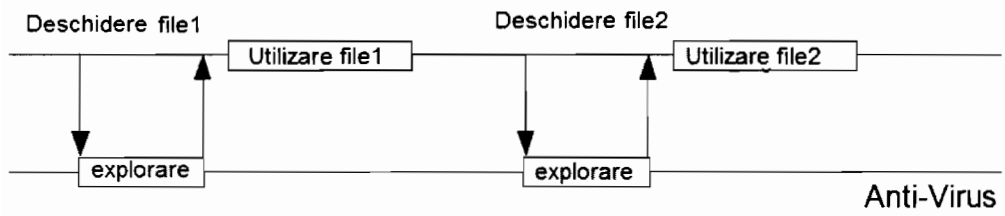

Figura 1 (stadiul tehnicii)

a-2013 00848--
29 -03- 2013

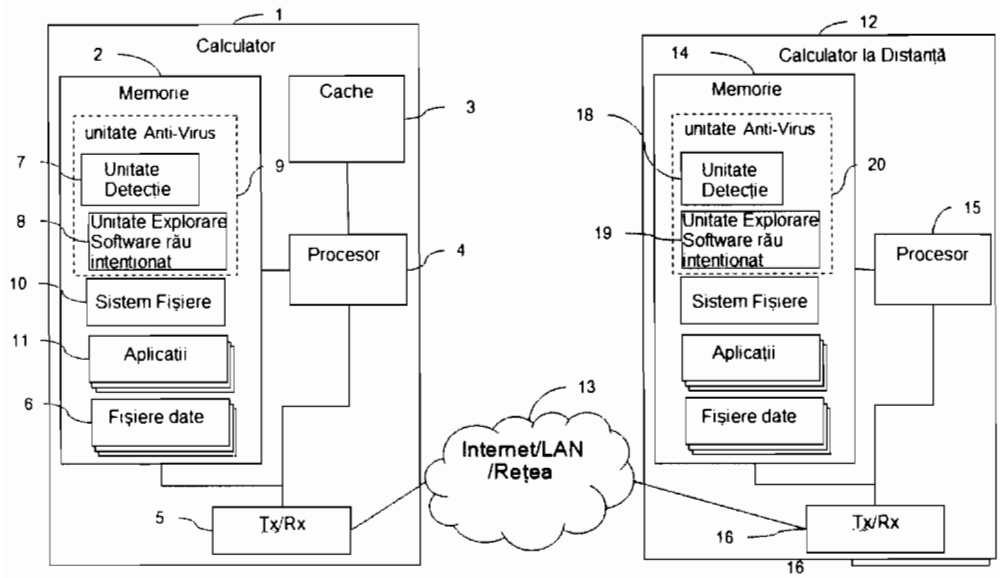

Figura 2

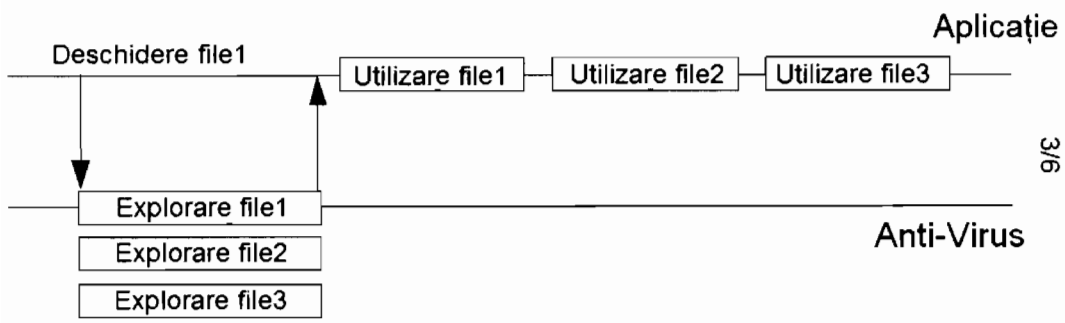
Aplicație
Deschidere file1
Utilizare file1
Utilizare file2
Utilizare file3
3/6
Explorare file1
Explorare file2
Explorare file3
Anti-Virus

Figura 3

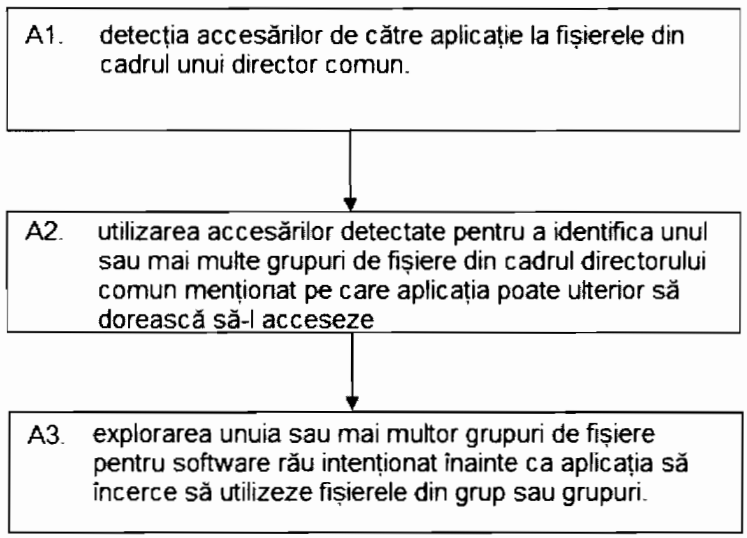

Figura 4

Drum Director	Listă de Extensii Accesate	Număr de reușite	Stare Element
C:\WINDOWS\system32	DLL, EXE	7	Colectat
C:\Program Files\Microsoft Office\OFFICE	EXE, DLL	3	Remarcat
C:\Program Files\Adobe\Reader 8.0\Resource\Font	PFB	10	Procesat

Figura 5

a-2013 00840--
29 -03- 2013

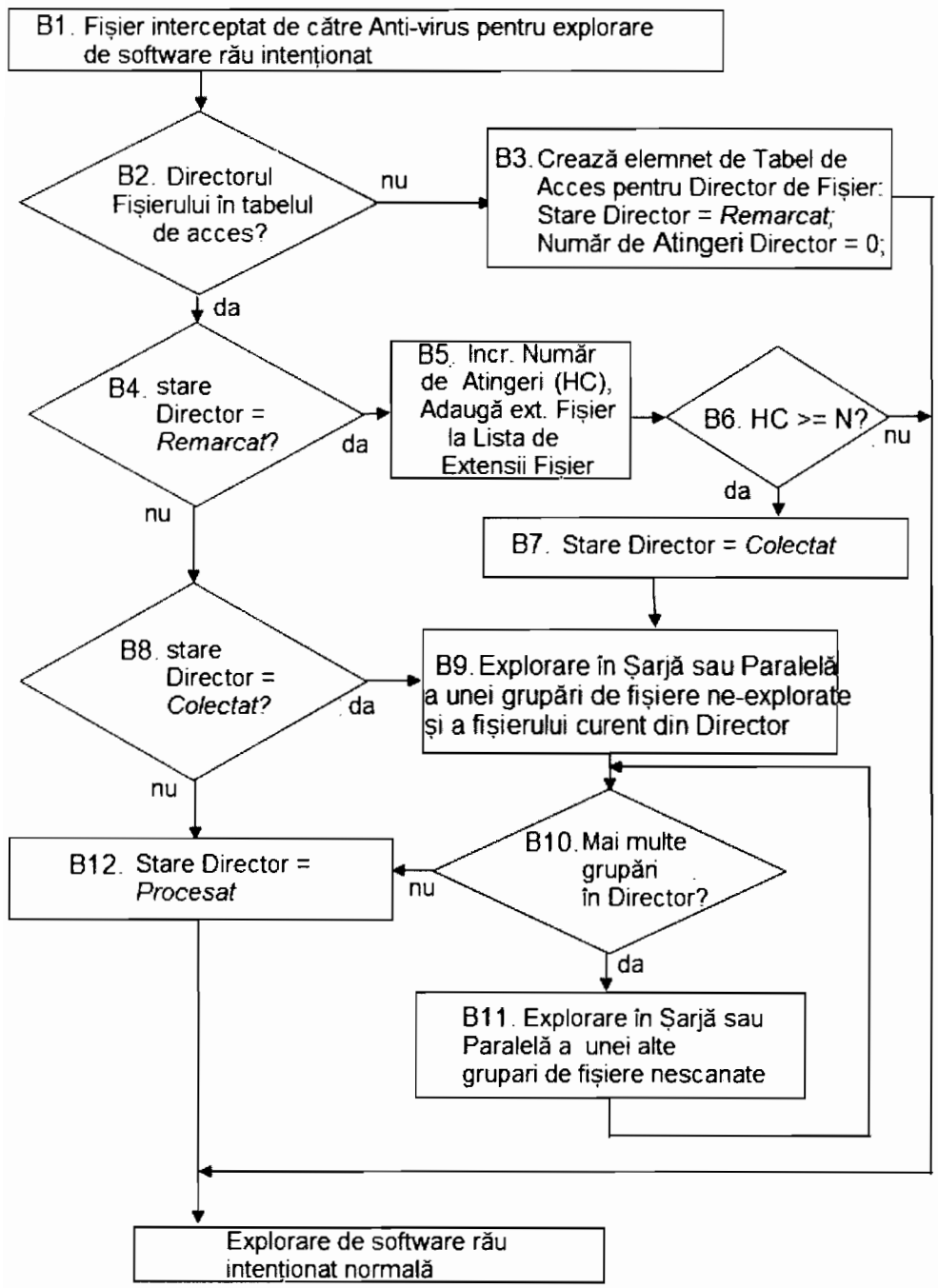

Figura 6

a-2013-00840--
29 -03- 2013

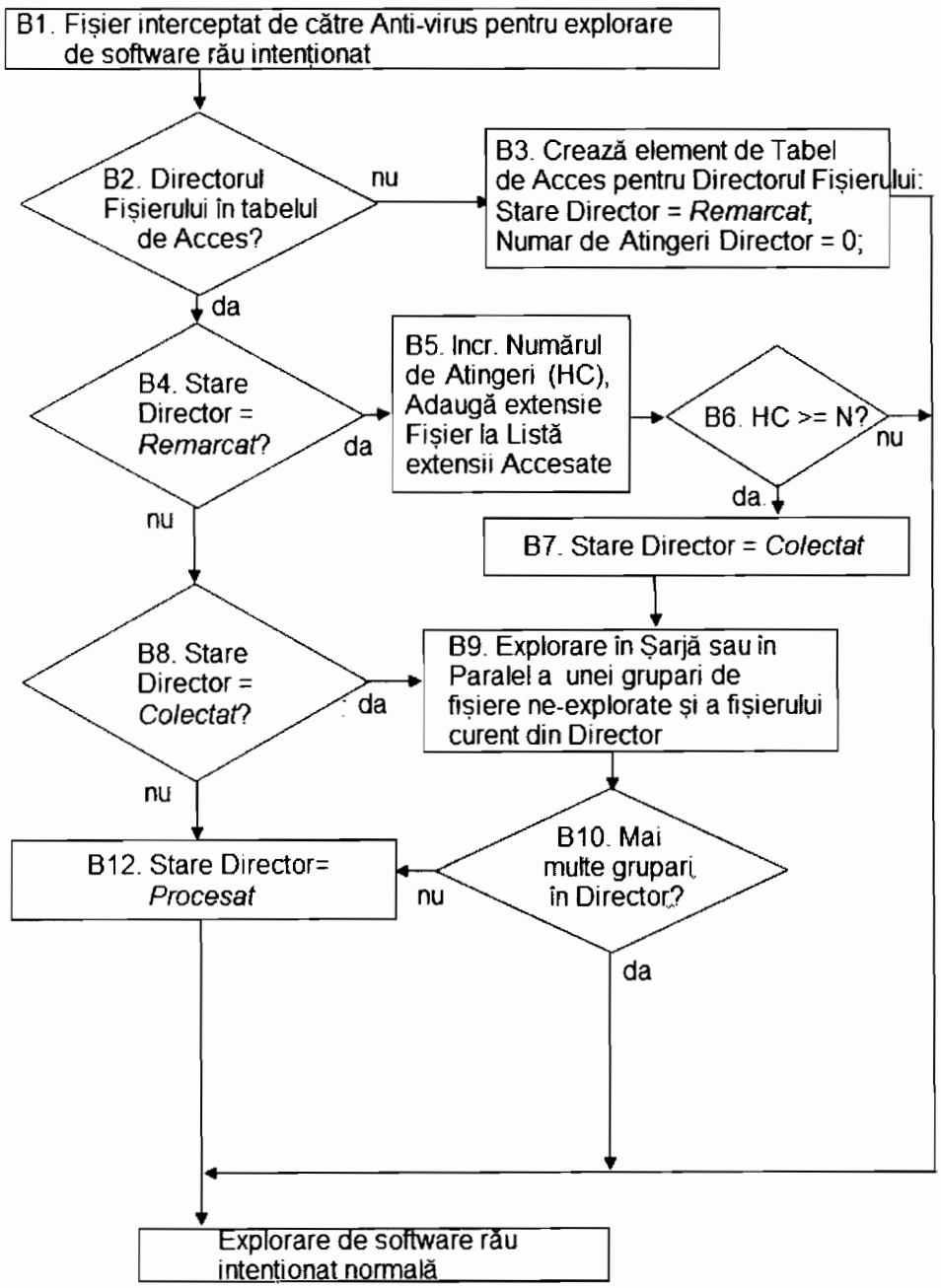

Figura 7