(19) OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 130379 B1**

(51) **Int.Cl.**
G06F 21/00 (2006.01)

(12) # BREVET DE INVENȚIE

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

(22) Data de depozit: **29/03/2012**

(45) Data publicării mențiunii acordării brevetului: **29/05/2020** BOPI nr. **5/2020**

(30) Prioritate:
16/05/2011 US 13/068610

(41) Data publicării cererii:
30/06/2015 BOPI nr. **6/2015**

(86) Cerere internațională PCT:
Nr. **EP 2012/055733 29/03/2012**

(87) Publicare internațională:
Nr. **WO 2012/156143 22/11/2012**

(73) Titular:
• **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

(56) Documente din stadiul tehnicii:
WO 2008/068240 A1; US 7681237

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

Examinator: **ing. MĂNĂILĂ MARIUS OCTAVIAN**

RO 130379 B1

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

În limba engleză termenul Malware este prescurtarea de la software rău intenționat (eng. malicious software), şi 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 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 şi oricare alte tipuri de software rău intenționat sau nedorit.

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

Software-ul antivirus în mod tipic furnizează explorarea fişierelor, la cerere, în care utilizatorul unui sistem de calculator determină când ar trebui să fie explorate fişierele 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 antivirus ca să exploreze dosare (eng. folders) sau directoare (aceşti termeni vor fi utilizați aici în mod interschimbabil) o dată pe săptămână, şi să exploreze toate fişierele de pe un sistem de calculator o singură dată pe lună. Suplimentar, software-ul antivirus 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 fişierelor în mod automat în fundal, atunci când există un acces detectat al fişierelor de către una sau mai multe aplicații care execută pe sistemul de calculator. Cea mai obişnuită metodă de acces la fişier este accesul de deschidere de fişier numai pentru citire. Acest tip de acces este comun pentru operațiuni pe fişiere multiple, de exemplu, la căutarea pentru/în fişiere, la pornirea şi în timpul execuției unei aplicații, la copierea fişierelor de la dosar la dosar (director la director), la comprimarea de fişiere etc. Următoarele exemple ilustrează suplimentar unele dintre aceste operațiuni obişnuite.

Exemplul 1, comanda copy (copiere):

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

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

- pentru fiecare fişier din c:\ source*.* deschide numai pentru citire fişierul curent (c:\ source\..);
- citeşte datele din fişier;
- închide fişierul;
- salvează datele la d:\dest\.

Comanda de copiere generează acces numai pentru citire continuu şi secvențial pentru toate fişierele sursă.

Exemplul 2. O aplicație care execută mai multe fișiere de modul: Se presupune faptul că aplicația constă dintr-un singur executabil (.EXE) şi un număr de module cum ar fi biblioteci legate în mod dinamic (dynamic linked libraries -.DLL). Atunci când un utilizator lansează aplicația, această aplicație încarcă bibliotecile necesare şi apoi începe execuția. Această operațiune ar putea fi reprezentată de către următorul pseudocod:

- pentru fişierele application.exe, module1.dll, module2.dll... moduleN.dll deschide numai pentru citire fişierul curent;
- încarcă datele din fişier.

Aplicația generează accesări de deschidere de fişier numai pentru citiri continue şi secvențiale pentru fişierele sursă din aplicație şi/sau directoarele de modul relevante.

Modele similare de acces de deschidere de fişier numai pentru citire continuă şi secvențială de fişiere multiple dintr-un director dat pot fi găsite în alte comenzi sau aplicații, de exemplu, căutarea unui model într-o colecție de fişiere (grep.exe sau findstr.exe), calculul unui şir de octeți de comprimare (eng. hash) peste fişiere (md5.exe), împachetarea într-un container (rar.exe sau winzip.exe) şi aşa mai departe.

O interacțiune obişnuită este ilustrată în fig. 1, între o aplicație şi software antivirus, atunci când aplicația efectuează un acces de deschidere de fişier numai pentru citire de fişiere multiple. În timpul operațiunii, numai atunci când software-ul antivirus detectează accesul de către aplicație la fişiere, acesta efectuează explorarea la acces a fişierelor.

În particular, atunci când aplicația încearcă să deschidă un fişier, solicitarea de deschidere este interceptată de către un filtru care generează o solicitare de explorare pentru utilizare de către software-ul antivirus, şi împiedică aplicația să deschidă şi să utilizeze fişierul. La recepția solicitării de explorare, software-ul antivirus explorează fişierul şi generează un rezultat în modalitatea obişnuită. În dependență de rezultat, accesul fişierului este înmânat înapoi la aplicație pentru utilizarea sa, de exemplu, citirea, copierea sau execuția fişierului. Cu toate acestea, dacă fişiere multiple au nevoie să fie accesate de către aplicație, această operațiune va fi repetată în mod secvențial pentru fiecare acces de fişier ulterior de către aplicație, aşa cum este prezentat în fig. 1. Acesta este un proces foarte lent şi laborios, ce are un impact asupra performanței aplicației şi 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 şi cum ar apărea în mod simultan. Un fir de execuție 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 ce are fire de execuție multiple, în care firele sunt planificate pentru a fi executate de către un sistem de operare în acelaşi timp. **Articolul INTEL™, *„Predicția şi măsurarea performanței paralele"* (*„Predicting and Measuring Parallel Performance"*), 9 martie 2010**, disponibil de la http://software.intel.com/en-us/ articles/predictinq-and-measurinq-parallel-performance/, descrie dezvoltarea de software paralelizat de către aplicații cu fire de execuție multiple, pentru a permite 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 divizarea 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 şi 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 acelaşi moment de timp (în dependenţă de numărul de procesoare), cu fiecare procesor sau nucleu executând un fir sau o sarcină particular/particulară. Cu scopul de a obţine performanţă maximă, aplicaţiile, atunci când sunt executate pe sistemul de calculator, ar trebui să încerce să blocheze ecuaţiile sau sarcinile complexe ale acestora.

Explorarea în paralel a mai multor fişiere pentru software rău intenţionat cu software antivirus poate fi realizată prin planificarea în mod simultan a uneia sau mai multor fire, pentru a trata procesul de explorare al fiecăruia dintre fişiere. Aşa cum s-a menţionat mai sus, sistemul de operare gestionează execuţia firelor pe un sistem de calculator cu sarcini multiple şi/sau nuclee multiple. Explorarea paralelă poate fi efectuată pe fişiere multiple într-o coadă de explorare, pentru a creşte performanţa sistemului de calculator. Organizarea în coadă de aşteptare a fişierelor accesate pentru explorarea de software rău intenţionat poate utiliza puterea explorării paralele. Astfel de explorare ar putea fi efectuată de către metode de explorare la închidere asincrone. Dar, chiar şi cu suportul de nucleu multiplu, explorarea paralelă la acces a fişierelor multiple pentru software rău intenţionat, în timpul accesului de deschidere de fişier numai pentru citire de către o aplicaţie, este problematică. Organizarea fişierelor în cozi de aşteptare pentru o explorare mai târziu paralelă sau în serie nu este o opţiune pentru aplicaţii care necesită operaţiunea de acces de deschidere de fişier numai pentru citire. Acest tip de acces la fişier necesită un răspuns sincron imediat de la software-ul antivirus, pentru a permite aplicaţiei să continue cât mai rapid posibil. Solicitările de explorare de la driverul (software specializat pentru acces la hardware) de filtrare la antivirus nu pot fi organizate în coadă pentru procesare de grup viitoare, deoarece software-ul antivirus nu cunoaşte fişierul următor pe care o aplicaţie îl va solicita.

Aplicaţiile pot genera solicitări de deschidere de fişier numai pentru citiri secvenţiale multiple arbitrare, şi logica de explorare antivirus tipică solicită ca fiecare solicitare de deschidere de fişier numai pentru citire să declanşeze un eveniment de explorare sau o solicitare pentru acel fişier. Din cauza naturii secvenţiale a accesului la fişier, logica de explorare nu poate determina care fişiere vor fi ulterior accesate de către aplicaţie. Acest lucru nu permite software-ului antivirus să profite de efectuarea de explorare în şarjă sau în paralel de fişiere multiple pe sisteme de calculator moderne. Acest lucru înseamnă faptul că aplicaţia va avea nevoie fie să aştepte până când explorarea pentru software rău intenţionat se termină pe toate fişierele înainte de a începe, fie să fie întreruptă în timpul execuţiei, în timp ce fiecare fişier care trebuie să fie accesat este explorat. Ambele scenarii deteriorează în mod semnificativ performanţa aplicaţiei şi a sistemului de calculator.

Procesul sincron de explorare la acces blochează o aplicaţie de a începe sau de a întrerupe execuţia aplicaţiei până când o explorare pentru software rău intenţionat pentru toate fişierele sau pentru fiecare fişier a fost efectuată. Astfel, software-ul antivirus împiedică execuţia aplicaţiei să progreseze, încetinind rata la care aceasta îşi poate îndeplini sarcinile. Acest lucru are un impact asupra performanţei sistemului de calculator.

Dezavantajul major al sistemelor antivirus existente constă în pierdere de performanţă prin scanare în timpul accesării fişierului/ fişierelor.

Problema tehnică pe care o rezolvă invenţia constă în minimizarea întârzierilor, în timpul executării aplicaţiilor, cauzate de scanarea fişierului/fişierelor în directorul comun.

Metoda de explorare împotriva software-ului rău intenţionat în timpul execuţiei unei aplicaţii pe un sistem de calculator cuprinde:

- întreţinerea unui tabel de acces la director pentru urmărirea accesului fişierelor din interiorul unui director comun, care este accesat de către aplicaţie, unde tabelul de acces la director include drumul directorului care menţine un nume sau o locaţie logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicaţie, şi o stare de acces care indică dacă directorul comun este în una dintre stările următoare: starea de pre-explorare, starea de explorare şi starea de explorat;

- detectarea accesărilor de către aplicație a fişierelor din cadrul directorului comun, şi actualizarea numărului de atingeri;

- modificarea stării de acces a directorului comun de la starea de pre-explorare la o stare de explorare atunci când numărul de atingeri atinge un prag predeterminat;

- utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun pe care aplicația poate ulterior dori să le acceseze în timpul execuției aplicației;

- declanşarea de explorare paralelă sau în şarjă a unuia sau mai multor grupuri de fişiere, împotriva software-ului rău intenționat, în timpul execuției aplicației, şi înainte ca aplicația să încerce să acceseze fişierele grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului curent detectat, pentru a fi accesat de către aplicație la unul sau mai multe grupuri de fişiere pentru explorare atunci când fişierul curent necesită explorare; şi

- actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

Programul de calculator pentru explorarea software-ului rău intenționat în timpul execuției unei aplicații pe un sistem de calculator cuprinde mijloace de cod de program de calculator adaptate pentru a efectua paşii următori:

- întreținerea unui tabel de acces la director pentru urmărirea accesului fişierelor din interiorul unui director comun care este accesat de către aplicație, unde tabelul de acces la director include drumul directorului care menține un nume sau o locație logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicație, şi o stare de acces care indică dacă directorul comun este în una dintre situațiile: starea de pre-explorare, starea de explorare şi starea de explorat;

- detecția accesărilor de către aplicație la fişierele din cadrul directorului comun, şi actualizarea numărului de atingeri;

- modificarea stării de acces a directorului comun de la starea de pre-explorare la o stare de explorare atunci când numărul de atingeri atinge un prag predeterminat;

- utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere în cadrul directorului comun, în timpul execuției aplicației, pe care aplicația poate ulterior să dorească să le acceseze;

- instruirea explorării paralele sau în serie a acelui unul sau a acelor mai multe grupuri de fişiere menționate, împotriva software-ului rău intenționat, în timpul execuției aplicației, înainte ca aplicația să încerce să acceseze fişiere ale grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului curent detectat pentru a fi accesat de către aplicație la cele unul sau mai multe grupuri de fişiere pentru explorare, atunci când fişierul curent necesită explorare; şi

- actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat, atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

Sistemul de calculator configurat pentru a explora fişiere împotriva unui software rău intenționat, în timpul execuției unei aplicații pe un procesor, şi pentru a întreține un tabel de acces la director pentru urmărirea accesului fişierelor din interiorul unui director comun, care este accesat de către aplicație, unde tabelul de acces la director include drumul directorului care menține un nume sau o locație logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicație, şi o stare de acces care indică dacă directorul comun este în una dintre starea de pre-explorare, starea de

explorare şi starea de explorat, cuprinde o unitate de detecție pentru detecția accesărilor de către aplicație a fişierelor din cadrul directorului comun, actualizarea numărului de atingeri, modificarea stării de acces a directorului comun de la starea de pre-explorare la starea de explorare, atunci când numărul de atingeri atinge un prag predeterminat, şi utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun, în timpul execuției aplicației, pe care aplicația ar putea dori ulterior să le acceseze, instruirea unei unități de explorare pentru explorarea paralelă sau în şarjă a unuia sau mai multor grupuri de fişiere menționate împotriva software-ului rău intenționat, în timpul execuției aplicației, înainte ca aplicația să încerce să acceseze fişierele grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a unui fişier curent detectat pentru a fi accesat de către aplicație la unul sau mai multe grupuri de fişiere pentru explorare, atunci când fişierul curent necesită explorare; şi actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat, atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

Prin aplicarea invenției se obțin următoarele avantaje:

- realizarea de scanări preventive ale unui/unor fişier/fişiere ce sunt necesare unor aplicații;
- îmbunătățirea sistemului de calcul.

Se dă, în continuare, un exemplu de realizare a invenției, în legătură cu fig. 1...7, ce reprezintă:

- fig. 1, diagramă care ilustrează un proces din stadiul tehnicii de efectuare a explorării de software rău intenționat la acces;
- fig. 2, schema unui sistem de calculator în conformitate cu aplicații concrete ale invenției prezente;
- fig. 3, diagramă care ilustrează un proces de efectuare a explorării de software rău intenționat la acces, în conformitate cu o aplicație concretă a invenției prezente;
- fig. 4, diagramă de flux care ilustrează un proces în conformitate cu o aplicație concretă a invenției prezente;
- fig. 5, tabel de acces la director pentru utilizare în actualizarea şi întreținerea directoarelor accesate de către aplicații, în conformitate cu aplicații concrete ale invenției prezente;
- fig. 6, diagramă de flux care ilustrează un proces de efectuare a explorării de software rău intenționat la acces, pentru o aplicație care accesează fişiere în conformitate cu o aplicație concretă a invenției prezente;
- fig. 7, diagramă de flux care ilustrează un proces de efectuare a explorării de software rău intenționat la acces pentru o aplicație care accesează fişiere în conformitate cu o altă aplicație concretă a invenției prezente.

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 performanța sistemului de calculator.

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

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

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

Metoda include opțional faptul că utilizarea accesărilor detectate include pasul de determinarea a numărului de accesări detectate din cadrul directorului comun, şi utilizarea rezultatelor pentru a declanşa pasul de explorare a grupurilor, care sunt unul sau mai multe. De preferință, declanşarea 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 fişiere include pasul de adăugare a fişierului curent detectat pentru a fi accesat de către aplicație, la un grup de fişiere, atunci când pasul de explorare este declanşat. Opțional, determinarea numărului de accesări detectate include pasul de resetare a numărului de accesări detectate, atunci când o primă perioadă de timp a trecut, şi pasul de explorare nu a fost declanşat. Opțional, metoda 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 declanşat.

Metoda include opțional faptul că pasul de utilizare a accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere include pasul de întreținere a unei liste de tipuri de fişier a fişierelor detectate accesate, şi pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de selecție a fişierelor pe baza listei de tipuri de fişier. Selecția fişierelor include suplimentar punerea în corespondență a listei de tipuri de fişier a fişierelor accesate de către aplicație, cu tipurile de fişier ale fişierelor din cadrul directorului comun.

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

În conformitate cu un al doilea aspect al invenției prezente este furnizat un program de calculator pentru explorarea pentru un 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 paşii următori:

- detecția accesărilor de către aplicație la fişiere din cadrul unui director comun;
- utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun menționat, pe care aplicația poate ulterior să dorească să le acceseze; şi
- instruirea unui explorator de software rău intenționat, pentru explorarea unuia sau mai multor grupuri de fişiere menționate pentru un software rău intenționat, înainte ca aplicația să încerce să acceseze fişierele 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 fişiere pentru un software rău intenționat.

În conformitate cu un al treilea aspect al invenției prezente, este furnizat un program de calculator aşa 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 fişiere pentru un 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 fişiere din cadrul unui director comun, şi utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun menționat, pe care aplicația ar putea ulterior să vrea să le acceseze, şi instruirea unei unități de explorare pentru explorarea unuia sau mai multor grupuri de fişiere menționate pentru un software rău intenționat, înainte ca aplicația să încerce să acceseze fişierele grupului sau grupurilor. Sistemul de calculator poate include suplimentar o unitate de explorare pentru efectuarea explorării grupurilor de fişiere, care sunt unul sau mai multe.

Cu scopul de a depăşi 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 şarjă sau în paralel de fişiere multiple, înainte ca o aplicație să utilizeze unul dintre fişierele multiple. Acest lucru semnifică faptul că execuția aplicației nu este în întregime blocată în accesări de fişier ulterioare. Aşa cum s-a descris anterior, explorarea în şarjă sau în paralel este planificarea simultană a unui grup de fişiere pentru explorare de către un sistem de calculator; de exemplu, planificarea simultană de fire de explorare multiple, câte un fir pentru fiecare fişier din grup, pentru execuție pe sistemul de calculator.

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

Prin efectuarea de explorare în şarjă sau în paralel a unui grup de fişiere pe care aplicația le poate utiliza, şansele ca aplicația să fie blocată sau întreruptă în mod continuu de către o explorare de software rău intenționat este minimizată. Acest lucru apare deoarece aplicația poate accesa şi utiliza fişierele explorate dintr-un grup, care acum nu necesită explorare. De fapt, dacă grupul corect de fişiere este identificat pentru fiecare explorare, va exista numai o întârziere a unei explorări de fişier şi, după aceea, execuția aplicației nu ar trebui să fie blocată de către nicio explorare de software rău intenționat suplimentară, atunci când aplicația accesează fişierele explorate. Acest tip de explorare în şarjă sau în paralel minimizează întârzierea introdusă de către explorarea de software rău intenționat la acces, astfel optimizând performanța sistemului de calculator.

Fig. 2 ilustrează schematic un sistem **1** de calculator şi un sistem **12** de calculator la distanță, în conformitate cu aplicații concrete ale invenției prezente. Sistemul **1** de calculator poate fi implementat ca o combinație de hardware şi software de calculator. Sistemul **1** de calculator cuprinde o memorie **2**, o memorie **3** intermediară, cu acces rapid (cache), un procesor **4** şi un emițător-receptor **5**. Memoria **2** stochează toate fişierele necesare pentru sistemul **1** de calculator. Fişierele stocate în memoria **2** includ diverse programe/fişiere executabile care sunt implementate de către procesorul **4**, precum şi oricare fişiere **6** de date.

Aplicațiile/programele/fişierele executabile stocate în memorie **2**, şi implementate de către un procesor **4**, includ o unitate **7** de detecție şi o unitate **8** de explorare de software rău intenționat, fiecare dintre acestea putând fi subunități ale unei unități **9** antivirus care pot executa software antivirus local, precum şi sistemul **10** de fişiere şi oricare alte programe/aplicații **11**. Fişierele **6** de date stocate în memoria **2** pot include fişiere de date de aplicație, tabele de acces la director, aşa cum sunt definite aici, fişiere de date de definiție de software rău intenționat, fişiere care conțin reguli de analiză euristice, liste albe, liste negre etc. Memoria **3** cache furnizează o unitate de stocare temporară, pentru stocarea de date care trebuie să fie explorate de către unitatea **8** de explorator de software rău intenționat. Emițător-receptorul **5** poate fi utilizat pentru a comunica peste o rețea **13** internet/LAN cu un sistem **12** de calculator la distanță. Sistemul **12** de calculator la distanță poate furniza stocare de date şi servicii de aplicație la un sistem **1** de calculator. De exemplu, sistemul **12** de calculator la distanță poate fi un server de aplicație care furnizează aplicații de tipul Software ca un Serviciu (Software as a Service - SaaS) la utilizatorul sistemului **1** de calculator.

Sistemul **12** de calculator la distanță este în mod tipic operat de către un furnizor de diverse aplicații care sunt executate pe sistemul **12** la distanță, şi utilizate la distanță de către utilizatorul sistemului **1** de calculator. Sistemul **12** de calculator la distanță poate fi implementat ca o combinație de hardware şi software de calculator, cum este pentru sistemul **1** de calculator. Sistemul **12** de calculator la distanță cuprinde o memorie **14**, un procesor **15**, şi un emițător-receptor **16**. În privința sistemului **1** de calculator, memoria **14** poate stoca fişiere care includ diverse aplicații/programe/fişiere executabile care sunt implementate de către un procesor **15**, precum şi oricare fişiere **16** de date. Aplicațiile/programele/fişierele executabile stocate în memoria **14**, şi implementate de către procesorul **15,** de asemenea, includ o unitate **18** de detecție şi o unitate **19** de explorator de software rău intenționat, fiecare dintre acestea putând fi subunități ale unei unități **20** antivirus care execută software-ul antivirus local pe sistemul **12** la distanță. Emițător-receptorul **16** este utilizat pentru a comunica astfel cu sistemul **1** de calculator peste rețeaua **13**.

În operațiune utilizatorul sistemului **1** de calculator poate executa aplicații local, sau poate executa aplicații pe sistemul **12** de calculator la distanță. Unitatea **8** de explorator pentru software rău intenționat a sistemului **1** de calculator poate fi utilizată pentru a explora fişiere locale pentru un software rău intenționat din memoria **2**, accesate de către aplicații locale. Unitatea **19** de explorator de software rău intenționat a sistemului **12** la distanță poate fi utilizată pentru a explora fişiere pentru software rău intenționat în memoria **14,** accesată de către aplicațiile sistemului **12** la distanță. Metodele de explorare a fişierelor 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, aşa cum sunt descrise aici, pot fi implementate în sisteme de calcul independente sau legate la rețea prin intermediul sistemelor de calcul distribuite, unde fişierele şi aplicațiile sunt stocate şi executate la distanță.

În particular, sistemele **1**, **12** de calculator sunt configurate pentru a explora fişierele pentru software rău intenționat în timpul execuției unei aplicații sau a aplicațiilor care se execută pe oricare dintre procesoarele **4**, **15** în mod corespunzător. Sistemele **1**, **12** de calculator includ unitățile de detecție **7**, **18**, în mod corespunzător, pentru detecția accesărilor de către aplicație la fişierele din cadrul unui director comun, şi utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun menționat, pe care aplicația poate să dorească să le acceseze ulterior, şi instruirea unităților **8**, **19** de explorare, în mod corespunzător, pentru explorarea unuia sau mai multor grupuri de fişiere menționate pentru un software rău intenționat, înainte ca aplicația să încerce să

acceseze fişierele grupului sau grupurilor. Aşa cum este ilustrat, sistemele **1**, **12** de calculator deja includ unitățile **8**, **19** de explorare, pentru explorarea unuia sau mai multor grupuri de fişiere menționate ca răspuns la instruirea unităților **7**, **18** de detecție, în mod corespunzător. Trebuie să fie apreciat faptul că, deşi explorarea unităților **8**, **19** este implementată în cadrul unităților **9**, **20** antivirus, în mod corespunzător, unitățile **8**, **9** de explorare ar putea fi de asemenea implementate pe alte sisteme de calculator/servere, astfel încât unitatea **7** sau **18** de detecție trimite instrucțiuni peste rețeaua **13,** pentru a avea grupurile de fişiere, 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 **12** de calculator la distanță, şi accesează fişiere de la un centru de date la distanță (nu este prezentat) unde detecția accesărilor de fişier este efectuată la centrul de date, dar explorarea de software rău intenționat este efectuată la sistemul **12** de calculator la distanță. Sistemul **12** de calculator la distanță poate efectua explorare de „Nor", care este un exemplu de furnizare a capacității de explorare pentru un software rău intenționat, peste o rețea sau un sistem de calculator distribuit. Pentru a minimiza suprasarcina implicată în explorarea fişierelor peste o rețea, adică minimizarea lățimii de bandă, explorarea poate fi limitată la verificarea meta-datelor de fişier stocate în centrul de date la distanță (serverul la distanță sau partea de susținere (backend)). Meta-datele ar putea fi create pentru fiecare fişier de la un şir de octeți de comprimare (hash) (de exemplu, shal), calculat de la datele fişierului sau de la porțiuni specifice ale datelor fişierului. Numai meta-datele sunt încărcate şi explorate de către sistemul **12** de calculator la distanță atunci când acesta detectează accesări generate de către o aplicație de utilizator la fişiere. Sistemul **1** de calculator gazdă al utilizatorului ar putea interoga sistemul **12** de calculator la distanță în legătură cu datele fişierului explorat, şi recepționează starea pe baza unei explorări de verificare limitate (curățare, nume fişier infectat şi software rău intenționat).

Aplicațiile concrete ale invenției permit explorarea paralelă (de exemplu, explorare cu fire multiple) pe un sistem **1** de calcul sau sistem **14** de calcul la distanță, pentru solicitări de explorare cum ar fi solicitări de explorare la acces de deschidere de fişier 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 fişiere multiple dintr-un director de lucru curent al aplicației, sau un director comun. Termenul director comun se referă la aceeaşi locație logică din memorie (de exemplu, dispozitiv de disc) unde unul sau mai multe fişiere sunt stocate. Performanța este optimizată datorită faptului că aplicațiile accesează în mod comun mai multe fişiere din acelaşi dosar sau director. Dacă software-ul antivirus recunoaşte acest tip de model de comportament de aplicație atunci acesta poate efectua explorare în avans asupra unui grup de fişiere pe care aplicația poate ulterior dori să le acceseze sau să le utilizeze. Software-ul antivirus efectuează apoi explorare la acces pe grupuri de fişiere multiple pentru un software rău intenționat.

Fig. 3 ilustrează procesul de efectuare de explorare de software rău intenționat la acces în şarjă sau în paralel, în conformitate cu o aplicație concretă a invenției prezente. Software-ul antivirus grupează fişiere multiple împreună în dependență de comportamentul aplicațiilor care accesează fişierele, şi execută explorare de căutare în avans pe grupuri de fişiere multiple. Rezultatele explorărilor sunt memorate în cache şi, dacă aplicația accesează fişierul explorat prin căutare în avans, aceasta recepționează un răspuns de la memoria cache despre faptul că fişierul a fost explorat, şi poate continua să utilizeze fişierul.

În practică, explorarea normală de fişier este implementată în modul de utilizator şi software-ul antivirus interceptează accesările de fişier de nivel redus de către aplicație, şi trimite o solicitare de explorare la modul de utilizator. Aceasta este o operațiune scumpă şi necesită comutație de context (nucleu la mod de utilizator şi din nou înapoi). Trebuie să fie apreciat faptul că metodele de explorare, aşa cum sunt descrise aici, reduc apelurile înapoi de la aplicație la software-ul antivirus, care îmbunătățesc în mod considerabil performanța. De exemplu, software-ul antivirus are un driver de filtru de nucleu care interceptează aplicații care încearcă să acceseze sau să deschidă fişiere. Driverul de filtru de nucleu trimite o solicitare la modul de utilizator pentru a efectua o sarcină de explorare pe fişierul pe care o aplicație încearcă să-l acceseze. Serviciul de explorare care execută în modul de utilizator efectuează o explorare de software rău intenționat reală pe fişier, şi notifică rezultatele şi starea explorării înapoi la driverul de filtru de nucleu. Pe baza acestor rezultate driverul de filtru de nucleu permite sau respinge aplicației accesul la fişier.

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

Deşi explorarea în şarjă sau paralelă a unui grup de fişiere poate îmbunătăți în mod substanțial performanța generală a unei aplicații sau a aplicațiilor care execută pe un sistem de calcul, performanța este îmbunătățită în mod substanțial dacă grupul de fişiere explorate include numai acele fişiere care sunt necesare pentru aplicație/aplicații. Explorarea fişierelor care nu sunt utilizate de către o aplicație poate avea impact asupra performanței, cu excepția cazului în care acel fişier va fi utilizat de către o altă aplicație. De exemplu, dacă software-ul antivirus explorează în avans prea multe fişiere, care nu vor fi accesate de către oricare aplicație, atunci acesta numai reduce performanța generală deoarece resursele calculatorului sunt utilizate pentru explorarea fişierelor nenecesare. Următoarele aplicații concrete ale invenției prezente descriu metode pentru minimizarea explorărilor de fişier nenecesare, ceea ce maximizează performanța aplicației sau a aplicațiilor şi a sistemului de calcul.

Fig. 4 reprezintă o diagramă de flux care ilustrează suplimentar procesul de explorare pentru un 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 antivirus pentru fiecare aplicație care accesează fişiere din cadrul unui director comun sunt schițate după cum urmează:

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

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

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

Cu privire la pasul A1, detecția accesărilor de către aplicație la fişierele din cadrul directorului comun poate include recepția unei solicitări de explorare pentru explorarea unui fişier accesat de către aplicație (fişierul curent accesat), din cadrul directorului comun. Detecția accesului la fişier de către aplicație poate, de asemenea, include intercepția accesului la fişier realizată de către aplicație, generarea solicitării de explorare şi trimiterea solicitării de explorare, atunci când explorarea este solicitată, la software-ul antivirus, pentru explorare.

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

Cu scopul de a utiliza accesările detectate, şi pentru a declanşa explorarea grupului sau grupurilor de fişiere, pasul A2 poate include determinarea numărului de accesări detectate din cadrul directorului comun, şi utilizarea rezultatelor pentru a declanşa pasul de explorare a grupurilor, care sunt unul sau mai multe. Declanşarea explorării poate apărea 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 antivirus, şi comportamentul observat al acestuia la una sau mai multe aplicații care accesează fişierele din cadrul directorului comun. Fişierul curent detectat pentru a fi accesat de către una sau mai multe aplicații poate fi adăugat la grupul de fişiere. Acest lucru poate apărea înainte sau atunci când pasul de explorare este declanşat. Fişierul curent accesat poate corespunde la fişierul care corespunde la solicitarea de explorare recepționată. Fişierul curent este apoi adăugat la grupul de fişiere pentru explorare. Grupul de fişiere este explorat pe baza solicitării de explorare recepționate de către antivirus pentru fişierul 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, şi pasul de explorare nu a fost declanşat.

Aşa cum s-a explicat mai jos, utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere poate include întreținerea unei liste de tipuri de fişier ale fişierelor detectate accesate, şi pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de selecție a fişierelor pe baza listei de tipuri de fişier. Selectarea fişierelor include suplimentar punerea în corespondență a listei de tipuri de fişiere ale fişierelor accesate de către aplicație, cu tipurile de fişier ale fişierelor din cadrul unui director comun. Software-ul antivirus poate întreține o listă pentru fiecare director comun care are fişiere 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 fişiere poate include urmărirea numărului de accesări detectate şi, de la rezultate, declanşarea pasul A3. Declanşarea 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 fişiere pentru explorare poate include selecția fişierelor din cadrul directorului comun pe baza tipurilor de fişier 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 fişiere 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 perioadă de timp care justifică terminarea explorării directorului, atunci explorarea unuia sau mai multor grupuri de fişiere ar putea fi terminată pentru a evita procesarea nenecesară. Acest lucru poate apărea atunci când o a doua perioadă de timp a trecut după ce pasul de explorare a fost declanşat.

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 fişier ulterioare din director, software-ul antivirus poate explora în mod simultan o şarjă de fişiere selectate de la tipurile de fişier de explorare prevalente, sau de la tipul de fişier accesat şi fişierul curent accesat. Aşa cum s-a menționat anterior, explorarea în mod simultan poate fi realizată prin planificarea în mod simultan de fire de explorare multiple pentru explorarea fişierelor, adică explorarea în paralel sau în şarjă. Explorarea este declanşată odată ce numărul de accesări detectate atinge un prag.

Explorarea trebuie să fie efectuată pe un grup de fişiere dacă se detectează faptul că fişierul curent pe care o aplicație îl detectează este un fişier neexplorat. În acest caz, accesul de fişier este detectat sau interceptat de către un driver de filtru nucleu, care generează o solicitare de explorare care este recepționată de către software-ul antivirus pentru explorarea fişierului accesat curent. În locul explorării numai a fişierului neexplorat, antivirusul nu numai că explorează fişierul neexplorat care a fost accesat, ci, de asemenea, încarcă un grup sau grupuri de fişiere pentru explorare. Software-ul antivirus execută explorarea solicitării de explorare curente (solicitarea de explorare pentru fişierul curent accesat) şi, în mod simultan, planifică (sau execută) explorarea de mai multe „solicitări de explorare purtate în spate" a fişierelor de la o listă încărcată. Lista încărcată este o listă de fişiere generate de către antivirus care poate fi accesată de la director - aceasta poate include tipuri de fişier accesate în mod prevalent. Antivirusul încarcă o selecție de fişiere de la director pe baza listei încărcate.

De exemplu, dacă un director (sau un dosar) are fişierele A, B, C, D, E, atunci la momentul de timp la care fişierele A şi B au fost explorate se poate considera faptul că acest director a fost accesat în mod frecvent. Dacă C, D şi E au fost puse pe lista încărcată, atunci când explorarea este declanşată de către accesările frecvente, antivirusul încarcă fişierele C, D, E (A şi B sunt omise deoarece acestea sunt deja explorate). Dacă se detectează faptul că fişierul C este accesat de către aplicație, atunci o solicitare de explorare pentru fişierul C va fie recepționată de către antivirus pentru explorare, care explorează fişierul C împreună cu explorarea fişierelor D şi E. Aceasta semnifică faptul că, atunci când fişierele D şi E sunt ulterior accesate de către o aplicație, solicitările de explorare pentru aceste fişiere nu vor fi generate de către driverul de filtru deoarece aceste fişiere au fost deja explorate.

Grupul sau grupurile de fişiere sunt fişiere selectate de la directorul pe care aplicație poate ulterior să vrea să le acceseze. Explorarea grupului sau grupurilor „duce în spate" explorarea fişierului accesat curent, adică duce în spate solicitarea de explorare a fişierului curent. Acest lucru împiedică solicitări de explorare viitoare, care sunt generate sau realizate pentru fişierele grupului.

Chiar dacă unele dintre fişierele selectate pentru explorare „dusă în spate" nu sunt accesate de către aplicație, pierderea de performanță într-o singură şarjă „dusă în spate" este neglijabilă datorită explorării în şarjă 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 creşte considerabil performanța generală. Software-ul antivirus estimează

multitudinea de fişiere care trebuie să fie accesate din director prin selecția fişierelor celor mai comune pe care aplicațiile le-au accesat din director peste o perioadă 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.

Fig. 5 reprezintă un tabel de acces la director care ilustrează actualizarea şi întreținerea accesărilor detectate de către aplicații la fişiere 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 antivirus pentru utilizare în determinarea numărului de ori de care fişierele din director sunt accesate.

Software-ul antivirus întreține tabelul de acces la director la momentul execuției (sau tabelul de acces la director), care urmăreşte accesul fişierelor în interiorul directoarelor de către aplicații. În această aplicație concretă, 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 fişiere sunt accesate;
- lista de extensii accesate, care conține o listă a extensiilor de fişier a fişierelor care au fost accesate şi explorate din director;
- numărul de atingeri, care prezintă numărul de accesări la fişier din director; şi
- starea elementului, care defineşte ciclul de viață al elementului directorului.

În această aplicație concretă, câmpul de Stare de Element are 3 stări logice: Remarcat, Colectat şi Procesat. Starea Remarcat (adică o stare de preexplorare) indică faptul că fişierul a fost accesat în director, dar că numărul de atingeri ale directorului nu este încă suficient pentru a garanta explorarea paralelă sau în şarjă. 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 şarjă. Software-ul antivirus preîncarcă grupuri de fişiere având extensii de fişier listate în Lista de Extensii Accesate, sau extensii de fişier ale fişierului curent care este accesat pentru explorare paralelă sau în şarjă. Starea Procesat semnifică faptul că explorarea cu căutare în avans a fost deja efectuată pentru director, şi fişierele 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 niciun fişier 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, şi serveşte pur şi simplu pentru a recunoaşte directoarele care pot fi accesate în mod frecvent. Stările Colectat şi Procesat au perioade mai lungi de valabilitate, datorită frecvenței accesărilor şi pentru a evita reexplorarea nenecesară a fişierelor accesate din director. Trebuie să fie apreciat faptul că aceste perioade pot fi variate de către software-ul antivirus pe baza oricărei scale de timp.

Este de apreciat faptul că respectivul câmp de Stare de Element este utilizat pentru a exclude reîncărcarea şi explorarea unui director dacă acesta a fost procesat numai recent (de exemplu, cu 10 min în urmă). Alte implementări ale tabelului de acces la director pot exclude acest câmp, şi 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.

Fig. 6 reprezintă o diagramă de flux care ilustrează suplimentar procesul de utilizare a tabelului din fig. 5 în efectuarea explorării de software rău intenționat la acces în paralel sau în şarjă, în conformitate cu o aplicație concretă a invenției prezente. Paşii metodei sunt efectuați de către software-ul antivirus după cum urmează:

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

B2. Verifică dacă directorul fişierului 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 fişier, şi inițializează Starea de Element a directorului la Remarcat, Numărul de Atingeri = 0, extensia de fişier a fişierului este adăugată la Lista de Extensii de Fişier (sau lista de tipuri de fişier explorată), continuă să efectueze explorare de software rău intenționat normală a fişierului 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 ce reprezintă numărul de accesări de fişier din director prin diverse aplicații, şi adaugă extensia de fişier a fişierului la Lista de Extensii Accesate.

B6. Verifică dacă Numărul de Atingeri (HC) ajunge la o valoare de prag N (de exemplu, HC >= N, unde A/=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 fişierul accesat.

B7. Starea de Element a directorului este modificată la starea Colectat, şi procesul continuă la pasul B8, unde software-ul antivirus încarcă un grup de fişiere care include fişierul accesat pentru explorarea în paralel sau în şarja 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 şarjă) pe un grup sau o selecție de fişiere neexplorate, care include fişierul curent din director.

Următoarele reguli pot fi utilizate pentru selecția unui grup de fişiere pentru explorarea în şarjă sau în paralel:

- selectează fişiere cu extensii sau tipuri de fişier care corespund la fişierul accesat în mod curent; sau
- selectează fişiere cu extensii sau tipuri de fişier listate în Lista de Extensii Accesate.

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

B11. Un alt grup de fişiere neexplorate este selectat din lista încărcată, şi o explorare de software rău intenționat în şarjă sau în paralel este efectuată; metoda continuă la pasul B10. Deşi software-ul antivirus 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 şi software-ul antivirus. Aceasta este explorarea în şarjă sau în paralel a fişierelor neexplorate suplimentare din listă, care ar putea fi efectuată în fundal astfel încât aplicația să poată continua.

B12. Deoarece nu mai există fişiere încărcate sau fişiere neexplorate având extensii de fişier 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 fişierului dacă este necesar.

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

Fig.7 reprezintă o diagramă de flux alternativă, care ilustrează explorarea de software rău intenționat la acces în şarjă sau în paralel, în conformitate cu o aplicație concretă a invenției prezente. Paşii de metodă de la B1 la B12 care sunt efectuați de către software-ul antivirus sunt similari cu cei ai fig. 6, cu excepția paşilor B10 şi B11 (B11 a fost eliminat). Pasul B10 este descris după cum urmează:

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

Motivul pentru necontinuarea de a efectua o explorare în paralel suplimentară a altor grupuri de fişiere este acela că aplicația are nevoie să acceseze numai un număr limitat de fişiere din director; acest proces împiedică software-ul antivirus de la efectuarea unei explorări în şarjă sau în paralel în fundal pe toate fişierele listate în Lista de Extensii de Acces, până când este absolut necesar, atunci când un alt fişier 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 fişiere de la un director comun. Sunt făcute următoarele presupuneri:

a) directorul comun are o colecție de fişiere *.exe şi *.dll;

b) tabelul de acces este întreținut de către programul antivirus;

c) tabelul de acces deja are un element de director în legătură cu directorul comun;

d) un număr de atingeri ce reprezintă numărul de accesări şi o listă de extensii de fişier accesate din directorul comun sunt întreținute.

Fluxul de logică este după cum urmează:

1. primele câteva fişiere „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 antivirus încarcă fişierele din director;

3. oricare solicitare de explorare următoare de fişiere „exe" din director declanşează o explorare „de ducere în spate" a altor fişiere „exe" (un grup de fişiere) 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 fişierele „exe" în mod secvențial, pentru a citi şi a copia date în celălalt director. Atunci când primul fişier „exe" este accesat de la directorul comun, o solicitare de explorare va fi generată pentru software-ul antivirus. Dacă directorul comun nu are un element de director în tabelul de acces, software-ul antivirus va crea şi va inițializa un element de director pentru directorul comun, numărul de atingeri al elementului de director ce reprezintă numărul de accesări de fişier este inițializat, şi tipul de fişier, 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, şi tipul de fişier „exe" este adăugat la lista de extensie dacă acesta nu este deja în lista de extensie.

Primul fişier „exe" accesat este apoi explorat în mod normal pentru software rău intenționat, şi utilizat de către comanda copy. Fişiere „exe" ulterioare sunt accesate, solicitări de explorare sunt realizate, şi sunt explorate normal de către software-ul antivirus, şi 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 antivirus începe să încarce sau determină unul sau mai multe grupuri de fişiere „exe" neexplorate de la directorul comun. Fiecare solicitare de explorare următoare a unui fişier „exe" neexplorat declanşează antivirusul pentru a efectua explorarea în paralel (adică în mod substanțial explorare simultană) a fişierului „exe" neexplorat şi a unuia dintre grupurile de fişiere neexplorate de la directorul comun. Explorarea continuă până când fişierele „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, şi este eliminat din tabelul de acces la expirare.

În ceea ce priveşte sistemele de calcul, aşa cum sunt descrise aici, fiecare poate efectua explorare în şarjă sau în paralel a unui grup de fişiere selectate dintr-o multitudine de fişiere 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 calculator să efectueze procedurile sau metodele aşa 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 nicio combinație specifică de circuite hardware şi/sau de software.

În particular, un program de calculator include mijloace de cod de program de calculator adaptate pentru a efectua paşii de detecție a accesărilor de către aplicație la fişierele din cadrul unui director comun, utilizând accesările detectate pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun menționat, pe care aplicația poate dori ulterior să le acceseze, şi instruind explorarea grupurilor de fişiere menționate, care sunt unul sau mai multe, pentru software rău intenționat, înainte ca aplicația să încerce să acceseze fişierele 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 fişiere menționate. Programul de calculator poate fi 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 şi hiper fire de execuție (hyper-threading) ale sistemelor de calculator moderne (aşa cum este descris aici şi, 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 fişier numai pentru citire, prin permiterea ca explorarea unuia sau mai multor grupuri de fişiere 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 împotriva unui software rău intenționat în timpul execuției unei aplicații pe un sistem de calculator, metoda cuprinzând:

- întreținerea unui tabel de acces la director, pentru urmărirea accesului fişierelor din interiorul unui director comun care este accesat de către aplicație, unde tabelul de acces la director include drumul directorului care menține un nume sau o locație logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicație, şi o stare de acces care indică dacă directorul comun este în una dintre următoarele stări: starea de preexplorare, starea de explorare şi starea de explorat;
- detectarea accesărilor de către aplicație a fişierelor din cadrul directorului comun, şi actualizarea numărului de atingeri;
- modificarea stării de acces a directorului comun de la starea de preexplorare la o stare de explorare atunci când numărul de atingeri ajunge la un prag predeterminat;
- utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun, pe care aplicația poate ulterior dori să le acceseze în timpul execuției aplicației;
- declanşarea de explorare paralelă sau în serie a unuia sau mai multor grupuri de fişiere, împotriva unui software rău intenționat, în timpul execuției aplicației şi înainte ca aplicația să încerce să acceseze fişierele grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului curent detectat pentru a fi accesat de către aplicație la unul sau mai multe grupuri de fişiere pentru explorare, atunci când fişierul curent necesită explorare; şi
- actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat, atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

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

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

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

5. Metodă în conformitate cu oricare dintre revendicările de la 1 la 4, în care pasul de utilizare a accesărilor detectate include pasul de determinare a numărului de accesări detectate în cadrul directorului comun, şi utilizarea rezultatelor pentru a declanşa pasul de explorare a acelui/acelor unul sau mai multe grupuri.

6. Metodă în conformitate cu revendicarea 5, în care pasul de declanşare a pasului de explorare apare atunci când numărul de accesări detectate atinge pragul predeterminat.

7. Metodă în conformitate cu revendicările 5 sau 6, în care utilizarea accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere include pasul de adăugare a fişierului curent detectat ca fiind accesat de către aplicație, la grupul de fişiere, atunci când pasul de explorare este declanşat.

8. Metodă în conformitate cu oricare dintre revendicările de la 5 la 7, în care determinarea numărului de accesări detectate include pasul de resetare a numărului de accesări detectate atunci când o primă perioadă de timp a trecut, şi pasul de explorare nu a fost declanşat.

9. Metodă în conformitate cu oricare dintre revendicările de la 5 la 8, în care pasul de explorare a unuia sau mai multor grupuri de fişiere 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 declanşat.

10. Metodă în conformitate cu oricare dintre revendicările de la 1 la 9, în care pasul de utilizare a accesărilor detectate pentru a identifica unul sau mai multe grupuri de fişiere include pasul de întreținere a unei liste de tipuri de fişier ale fişierelor detectate accesate, şi pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de selecție a fişierelor pe baza listei de tipuri de fişier.

11. Metodă în conformitate cu revendicarea 10, în care pasul de selecție a fişierelor include suplimentar punerea în corespondență a listei de tipuri de fişier a fişierelor accesate de către aplicație cu tipurile de fişier ale fişierelor din cadrul directorului comun.

12. Metodă în conformitate cu revendicările 10 sau 11, în care fişierele din cadrul grupului sau grupurilor de fişiere sunt fişiere din cadrul directorului comun care necesită explorare.

13. Metodă în conformitate cu oricare dintre revendicările de la 10 la 12, în care pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului curent detectat pentru a fi accesat de către aplicație, la un grup de fişiere pentru explorare.

14. Metodă în conformitate cu oricare dintre revendicările de la 1 la 13, în care pasul de detecție de accesări de către aplicație la fişierele din cadrul directorului comun include recepția unei solicitări de explorare pentru explorarea unui fişier accesat de către aplicație din cadrul directorului comun.

15. Metodă în conformitate cu revendicarea 14, în care pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului care corespunde la solicitarea de explorare la grupul de fişiere pentru explorare.

16. 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 paşii următori:

- întreținerea unui tabel de acces la director, pentru urmărirea accesului fişierelor din interiorul unui director comun care este accesat de către aplicație, unde tabelul de acces la director include drumul directorului care menține un nume sau o locație logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicație, şi o stare de acces care indică dacă directorul comun este în una dintre următoarele stări: starea de preexplorare, starea de explorare şi starea de explorat;
- detecția accesărilor de către aplicație la fişierele din cadrul directorului comun, şi actualizarea numărului de atingeri;
- modificarea stării de acces a directorului comun de la starea de preexplorare la o stare de explorare atunci când numărul de atingeri atinge un prag predeterminat;
- utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere în cadrul directorului comun în timpul execuției aplicației, pe care aplicația poate ulterior să dorească să le acceseze;
- instruirea explorării paralele sau în serie a acelui unul sau a acelor mai multe grupuri de fişiere menționate, împotriva unui software rău intenționat, în timpul execuției aplicației, înainte ca aplicația să încerce să acceseze fişiere ale grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a fişierului curent detectat pentru a fi accesat de către aplicație, la cele unul sau mai multe grupuri de fişiere pentru explorare, atunci când fişierul curent necesită explorare; şi

- actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat, atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

17. Program de calculator în conformitate cu revendicarea 16, care cuprinde suplimentar mijloace de cod de program de calculator adaptate pentru a efectua explorarea unuia sau mai multor grupuri de fişiere menționate împotriva unui software rău intenționat, ca răspuns la pasul de instruire.

18. Program de calculator în conformitate cu revendicarea 16 sau 17, încorporat pe un mediu care poate fi citit de calculator.

19. Sistem de calculator configurat pentru a explora fişiere împotriva unui software rău intenționat, în timpul execuției unei aplicații pe un procesor, şi pentru a întreține un tabel de acces la director, pentru urmărirea accesului fişierelor din interiorul unui director comun care este accesat de către aplicație, unde tabelul de acces la director include drumul directorului care menține un nume sau o locație logică a directorului comun, un număr de atingeri care indică numărul de accesări de fişier la directorul comun de către aplicație, şi o stare acces care indică dacă directorul comun este în una dintre stările următoare: starea de preexplorare, starea de explorare şi starea de explorat, sistemul de calculator cuprinzând:

- o unitate de detecție pentru detecția accesărilor de către aplicație a fişierelor din cadrul directorului comun, actualizarea numărului de atingeri, modificarea stării de acces a directorului comun de la starea de preexplorare la starea de explorare, atunci când numărul de atingeri atinge un prag predeterminat, şi utilizarea accesărilor detectate şi a numărului de atingeri pentru a identifica unul sau mai multe grupuri de fişiere din cadrul directorului comun în timpul execuției aplicației, pe care aplicația ar putea dori ulterior să le acceseze, instruirea unei unități de explorare pentru explorarea paralelă sau în serie a unuia sau mai multor grupuri de fişiere menționate, împotriva unui software rău intenționat, în timpul execuției aplicației, înainte ca aplicația să încerce să acceseze fişierele grupului sau grupurilor, unde pasul de identificare a unuia sau mai multor grupuri de fişiere include pasul de adăugare a unui fişier curent detectat, pentru a fi accesat de către aplicație, la unul sau mai multe grupuri de fişiere pentru explorare, atunci când fişierul curent necesită explorare; şi actualizarea stării de acces a directorului comun de la starea de explorare la starea de explorat, atunci când toate cele unul sau mai multe grupuri de fişiere identificate din directorul comun au fost explorate împotriva atacurilor de software rău intenționat.

20. Sistem de calculator în conformitate cu revendicarea 19, care cuprinde suplimentar o unitate de explorare pentru explorarea unuia sau mai multor grupuri de fişiere menționate, ca răspuns la instruirea de către unitatea de detecție.

21. Produs program de calculator care cuprinde cod de instrucțiuni, care, atunci când este executat pe un procesor, efectuează metoda în conformitate cu oricare dintre revendicările de la 1 la 15.

(51) Int.Cl.
G06F 21/00 (2006.01)

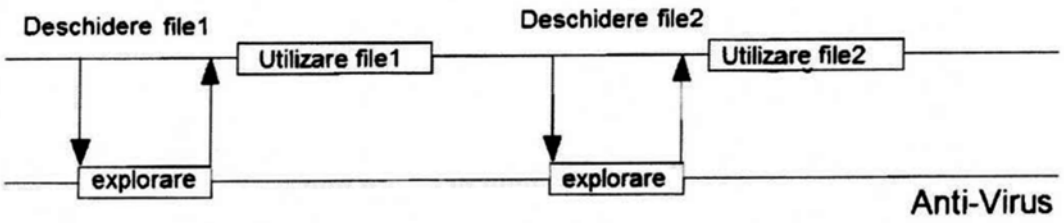

Fig. 1

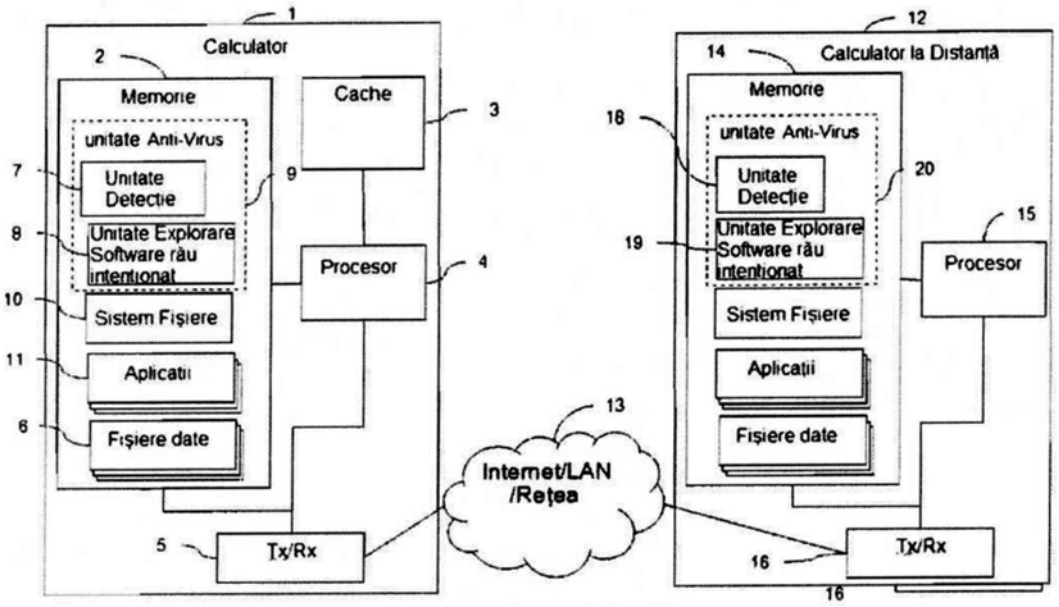

Fig. 2

(51) Int.Cl.
G06F 21/00 (2006.01)

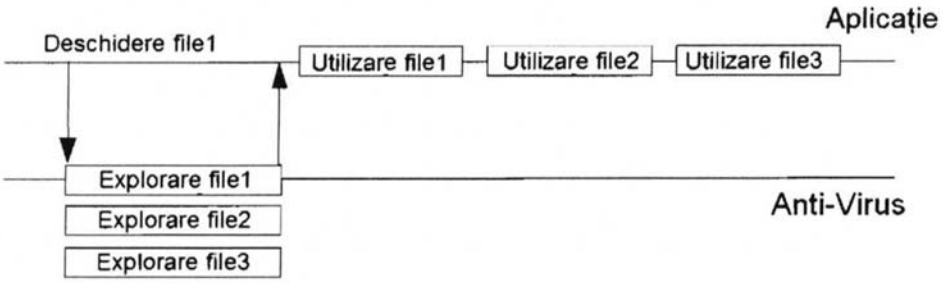

Fig. 3

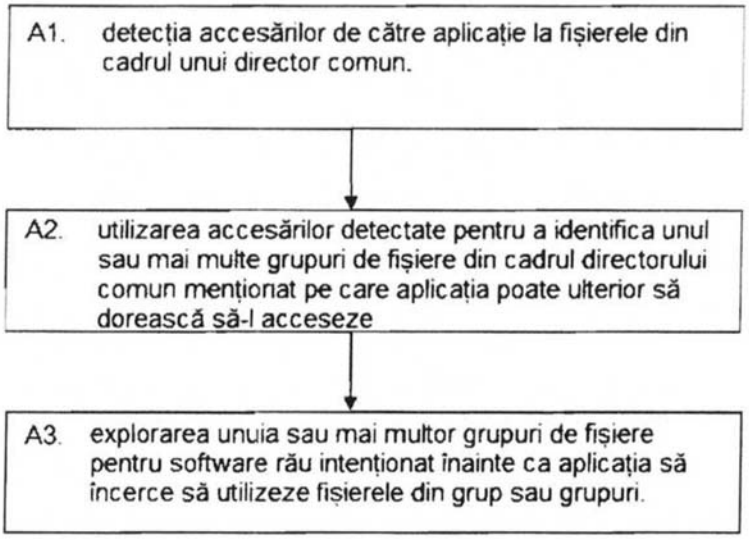

Fig. 4

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

Fig. 5

(51) Int.Cl.
G06F 21/00 (2006.01)

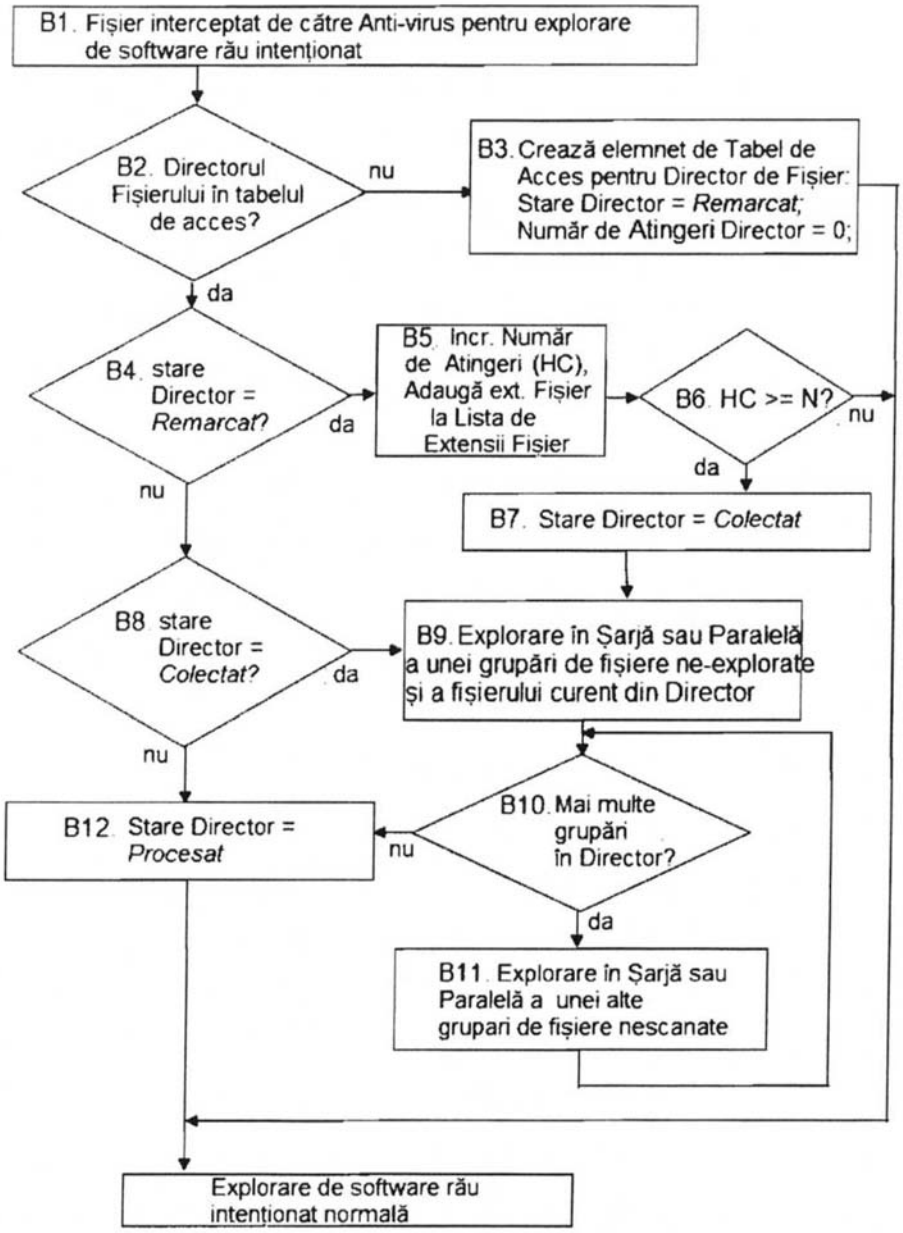

Fig. 6

(51) Int.Cl.
G06F 21/00 (2006.01)

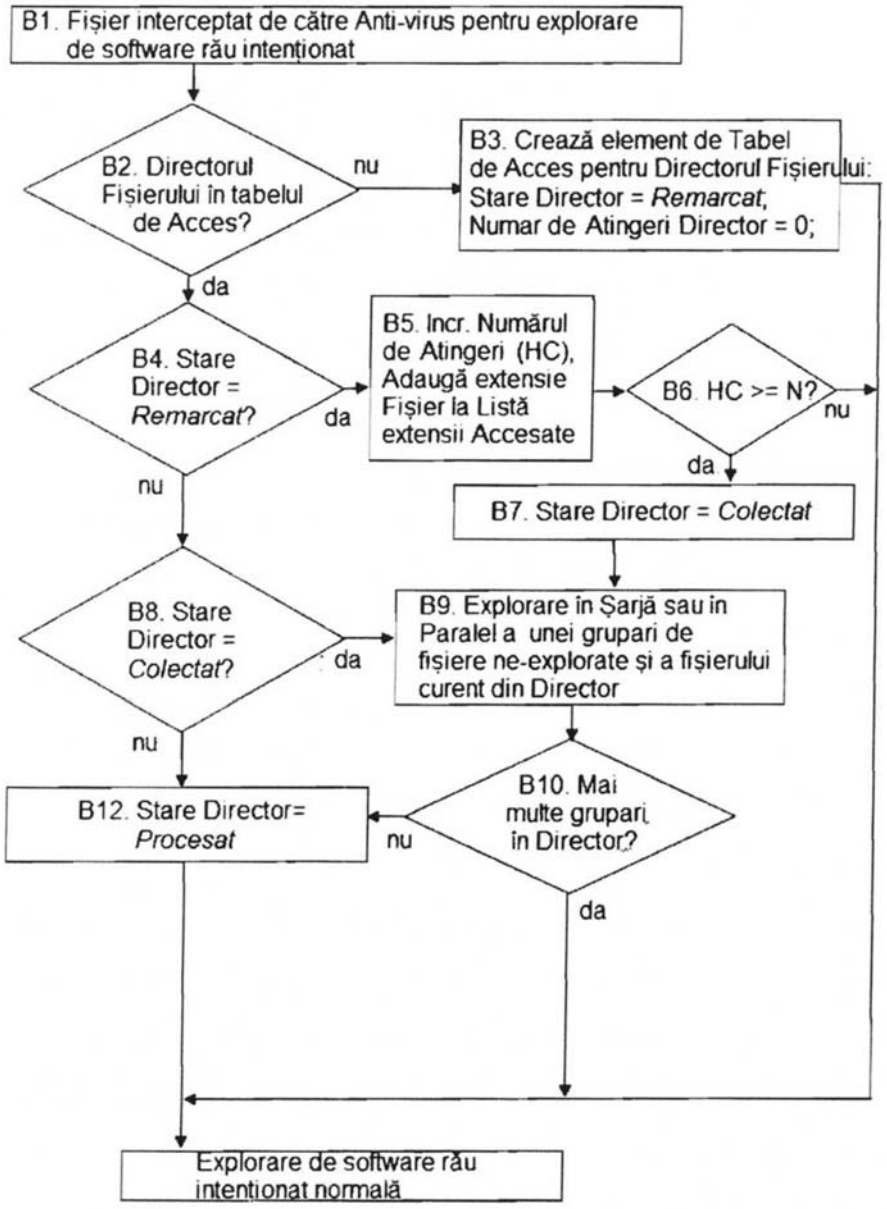

Fig. 7

Editare şi tehnoredactare computerizată - OSIM
Tipărit la: Oficiul de Stat pentru Invenţii şi Mărci
sub comanda nr. 204/2020