MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	**101997900605565**
Data Deposito	**20/06/1997**
Data Pubblicazione	**20/12/1998**

Titolo

PROCEDIMENTO PER LA PROTEZIONE DEI PERSONAL COMPUTER DAI VIRUS PRESENTI SUL BOOT SECTOR DI SUPPORTI DI MEMORIA NON VOLATILE QUALI FLOPPY-DISK, CD-ROM, DISCHI RIGIDI E SIMILI

Descrizione dell'invenzione industriale dal titolo: PROCEDIMENTO PER LA PROTEZIONE DEI PERSONAL COMPUTER DAI VIRUS PRESENTI SUL "BOOT SECTOR" DI SUPPORTI DI MEMORIA NON VOLATILE QUALI FLOPPY-DISK, CD-ROM, DISCHI RIGIDI E SIMILI; a nome di Laszlo Hegyi, cittadino ungherese residente presso il Pontificio Seminario Romano Maggiore, P.zza S. Giovanni in Laterano, 4 - ROMA.

*****

La presente invenzione riguarda il settore dei personal computer, e più in particolare la protezione di queste macchine dai virus informatici che possono venire introdotti tramite lo scambio di supporti di memoria non volatile.

Sono purtroppo ben noti i problemi che si possono riscontrare nel caso in cui il proprio personal computer, che nel seguito indicheremo semplicemente con PC, venga infettato da un virus. In questi casi infatti, oltre che ad avere problemi anche pesanti sul funzionamento della macchina, si possono anche avere difficoltà nell'eliminazione del virus stesso nonché nel recupero dei dati da esso danneggiati.

Attualmente, sono noti e diffusi svariati tipi di antivirus, che non sono altro che particolari

programmi da installare sui PC.

Detti programmi antivirus, in quanto tali, presentano sostanzialmente due grossi svantaggi: il primo è dato dal fatto che, ricorrendo all'uso di appositi database, possono subire l'azione di un virus diverso da quelli da essi memorizzati e riconosciuti, il secondo è dovuto al fatto che i programmi antivirus diventano ben presto obsoleti, perché quotidianamente vengono messi in circolazione nuovi e più potenti virus che non sono riconoscibili e/o eliminabili dagli antivirus installati sui PC.

Per questo motivo, è necessario aggiornare frequentemente l'antivirus presente sul proprio computer proprio per evitare di infettarsi con un nuovo virus.

Oltre a ciò, si deve tenere presente che esistono sostanzialmente due tipi di virus, i virus residenti nel "boot sector" dei supporti di memoria non volatile (floppy disk e CD-ROM), ed i virus residenti nei programmi eseguibili (quali ad esempio *.exe, *.com, *.sys, *.dll, etc.).

I virus presenti nei programmi eseguibili possono entrare in azione solo ed esclusivamente se e quando il programma che li contiene viene eseguito.

I virus presenti nel "boot sector" dei supporti

di memoria non volatile invece, sono i più pericolosi perché entrano in azione non appena l'utente effettua una semplice lettura del contenuto del supporto di memoria non volatile stesso, e l'utente non ha alcuna difesa né la possibilità di evitare di infettarsi.

Scopo del trovato è superare detti problemi e gli svantaggi degli antivirus attualmente noti fornendo un procedimento di difesa dai virus completamente diverso ed innovativo rispetto a quelli attuali, in grado di bloccare qualunque virus presente nel "boot sector" dei supporti di memoria non volatile.

Un altro scopo del trovato è quello di fornire una procedura antivirus installabile dal fabbricante, sotto forma di programma firmware, nel BIOS del PC rendendo il computer virtualmente inattaccabile dai virus del "boot sector" già dall'origine.

In sostanza, il procedimento antivirus secondo l'invenzione impedisce ai virus residenti nel "boot sector" di accedere al disco fisso del PC, facendo in modo che il programma di "boot sector" non abbia mai il controllo delle operazioni eseguite dal PC, e/o di installarsi in maniera residente in memoria.

Un PC attrezzato con la presente invenzione diventa completamente immune a tutti quei virus che

risiedono nel "boot sector" dei floppy disk, dei CD-ROM e di tutti quei supporti di memoria non volatile o "media" che, se infetti, una volta letti dal PC contagiano la macchina stessa.

Dal momento che, su un media o supporto di memoria, il virus può risiedere nel "boot sector" o nei files di tipo eseguibile contenuti nel media stesso, un PC attrezzato secondo il trovato diventa assolutamente e definitivamente inattaccabile dai virus informatici, semplicemente evitando di leggere programmi eseguibili non provenienti da fonte certa e/o non originali.

Considerando poi che la maggior parte dei files letti dagli utenti di PC sono di tipo non eseguibile, quali files di testo, dati, immagini, suoni, ecc., anche non seguendo l'accortezza citata poc'anzi il procedimento secondo il trovato è vantaggiosamente in grado di ridurre drasticamente il rischio di contagio dei PC.

Una migliore comprensione del trovato si avrà con la seguente descrizione dettagliata e con riferimento agli schemi a blocchi allegati.

Nei disegni:

le figure 1 e 2 mostrano lo schema a blocchi funzionale delle fasi essenziali previste dal

procedimento secondo il trovato.

Con riferimento alle figure allegate, nel seguito verrà descritto un procedimento che costituisce un forte passo avanti nella lotta ai virus informatici che affliggono i PC. Esso si basa su un principio completamente diverso da quello dei programmi antivirus oggi esistenti.

Il principio sul quale si basa la presente invenzione è di impedire al virus eventualmente presente nel "boot sector" di scrivere sul disco fisso, e/o di installarsi in maniera residente in memoria.

Per far questo, secondo il trovato, non si lascia mai il controllo delle azioni eseguite dal PC al programma di "boot sector".

Il procedimento che si descrive viene realizzato da un programma di tipo firmware, da implementare preferibilmente nel BIOS del computer, che agisce secondo il diagramma di flusso mostrato nelle figure 1 e 2 e che necessita dei seguenti files di appoggio e di lavoro:

FILE1: è sostanzialmente un BUFFER che contiene la condizione originale, ovvero quella prima del "booting", della memoria convenzionale ed eventualmente anche di

una parte di quella estesa;

FILE2: è un'area di memoria che agisce come una RAM simulata allo scopo di far lavorare il virus in questa RAM fittizia anziché in quella vera;

FILE3: è costituito da un'altra area di memoria e serve a simulare il disco fisso: il virus scrive su questo file invece che sul vero disco fisso;

FILE4: è costituito da un BUFFER atto a contenere i cambiamenti eventualmente apportati dal programma di "boot sector" al media sorgente.

I files 2, 3 e 4 sono inizialmente vuoti e vengono scritti solo nel caso in cui il virus tenti di scrivere sul supporto di memoria, sul disco fisso, e/o nella RAM in modo residente.

Detti files debbono essere costruiti nella RAM oppure sul disco fisso del PC.

Con il procedimento secondo l'invenzione, prima di leggere un supporto di memoria non volatile o media, vengono effettuate le seguenti operazioni:

1) bloccaggio di tutti gli INTERRUPT, affinché non ci siano interferenze durante il salvataggio della RAM convenzionale nel FILE 1;

2) salvataggio della RAM convenzionale nel FILE 1;

3) modificazione della tabella degli INTERRUPT, in modo tale che non sia possibile far partire un programma già residente in memoria;

4) rimozione del blocco degli INTERRUPT;

5) caricamento del "boot program" del supporto di memoria non volatile in memoria e nel FILE2;

6) controllo della prossima istruzione da eseguire presente nel "boot program";

7) verifica della pericolosità dell'istruzione trovata nel "boot program": se non lo è, si procede con la fase 8, altrimenti si passa alla fase 12;

8) settaggio dell'interrupt vector e del trapflag in modo che, dopo l'esecuzione dell'istruzione, il controllo torni alla procedura antivirus che si descrive;

9) esecuzione dell'istruzione giudicata non pericolosa;

10) cancellazione del trap flag;

11) nel caso detta istruzione non sia l'ultima si ritorna al passo n° 6, altrimenti si prosegue con il passo 13;

12) si eseguono una serie di istruzioni che fanno agire detta istruzione pericolosa sui files fittizi (FILE2÷FILE4) anziché sul vero disco fisso, poi si

prosegue con la fase 11;

13) si salvano i dati forniti dal "boot program" nel FILE4;

14) si ripristina il contenuto iniziale della RAM convenzionale tramite il FILE1;

15) nel caso in cui ci siano state operazioni pericolose si avverte l'utente della presenza di virus suggerendo di formattare il media (se è scrivibile), poi si consegnano i dati ottenuti, che si trovano nel FILE4, al sistema che può leggere il supporto di memoria;

16) si cancellano i files di lavoro e si termina la procedura antivirus.

E' importante notare che le istruzioni della fase 12 devono anche verificare che, nel caso in cui venga letto un campo già scritto precedentemente dal "boot program", detta lettura avvenga sul corrispondente file fittizio.

A questo punto, è necessario chiarire meglio cosa si intende per istruzione pericolosa.

E' da ritenersi rischiosa ogni istruzione che effettua una o più operazioni che intervengono direttamente sulla memoria e/o sul disco fisso, come ad esempio le seguenti:

- cancellazione di "trap flag",

- cambiamento del "trap interrupt" (indirizzo di memoria),
- scrittura sul disco fisso,
- installazione del "boot program" o di una sua parte in maniera residente,
- scrittura sul supporto di memoria non volatile sorgente,
- lettura di un campo già scritto precedentemente dal "boot program",
- scrittura in memoria.

Da quanto detto finora è chiaro come in presenza di virus, ovvero di programmi che cercano di effettuare operazioni illegittime, il procedimento secondo il trovato preserva dal contagio gli elementi del PC quali il disco fisso e la memoria, facendo vantaggiosamente lavorare il virus in maniera controllata, su un sistema fittizio costituito dai files di appoggio FILE2, ..., FILE4, e ripristinando lo stato iniziale soltanto dopo che la procedura di controllo ha dato l'autorizzazione.

Vantaggiosamente, anche in presenza di virus nel "boot program", i dati del supporto di memoria non volatile possono essere letti senza pericolo, e ciò è di estrema importanza per i media scrivibili una sola volta, perchè di fatto viene scritto tutto soltanto

nei files di appoggio.

Inoltre è possibile formattare un supporto di memoria non volatile o media contagiato e togliere il virus dal "boot sector" senza il pericolo che il virus possa attivarsi e reagire.

Si osservi che se un PC viene contagiato a causa di un virus proveniente da un codice eseguibile presente nel computer stesso, la procedura secondo il trovato non impedisce al virus di inserirsi nel "boot sector", ma detto virus non potrà entrare in un altro computer dotato della protezione che si descrive.

E' importante notare che se la procedura antivirus secondo l'invenzione è installata nel BIOS, è già attiva alla partenza del sistema e quindi impedisce l'attività di un eventuale virus che risiede nel "boot sector" del disco fisso o di un dischetto di sistema, anche se esso è nella penultima fase di attività, ovvero sta per iniziare a danneggiare i dati. Per questo, anche nel caso in cui il "boot program" del disco fisso venga contagiato da un codice eseguibile, il trovato protegge comunque i dati.

Il presente antivirus indaga volta per volta sulla provenienza dei virus in quanto non è attaccabile dai "boot virus" che possono essere

scritti da qualsiasi utente e diffusi con qualsiasi dischetto o supporto di memoria non volatile.

Poiché il virus pericoloso può venire solo da un codice eseguibile, è più facile rintracciarne la provenienza.

Come già accennato in precedenza, il procedimento antivirus che si descrive rileva la presenza dei virus senza dover ricorrere all'uso di appositi database, che per loro natura hanno bisogno di aggiornamento incessante, e occupano sempre maggior spazio. Dato che finché il modo di funzionamento del PC resta intatto il trovato non ha bisogno di essere aggiornato, quest'ultimo può essere considerato come la soluzione definitiva ai problemi relativi ai virus informatici da "boot sector", ed è da ritenersi efficace anche contro tutti i nuovi virus che vengono posti in circolazione successivamente all'installazione dell'antivirus stesso.

Vantaggiosamente, la procedura antivirus oggetto della presente invenzione è installabile, sotto forma di programma firmware, nel BIOS del PC dal fabbricante, che quindi è in grado di vendere computers già virtualmente inattaccabili dai virus.

Maurizio SARPI
dello
Studio FERRARIO

RIVENDICAZIONI

1. Procedimento per la protezione dei computer dai virus presenti nel "boot sector" di supporti di memoria non volatile, caratterizzato dal fatto di impedire ai virus eventualmente presenti sia di installarsi in memoria in modo residente che di accedere al disco fisso facendo in modo che il programma di "boot sector" non abbia mai il controllo delle operazioni eseguite dal computer; a tale scopo essendo prevista la creazione di uno spazio di memoria, volatile o non, atto a contenere sia una copia della memoria convenzionale del sistema reale originale che i cambiamenti eventualmente apportati dal virus sulla memoria convenzionale stessa, sul disco fisso e/o sui supporti di memoria non volatile; ottenendosi con ciò di salvaguardare il sistema reale simulando un sistema fittizio al virus di aver agito sul sistema reale stesso.

2. Procedimento di cui alla rivendicazione 1, caratterizzato dal fatto che la tabella degli INTERRUPT viene cambiata in modo tale da impedire ad altri eventuali programmi residenti di entrare in azione.

3. Procedimento di cui alle rivendicazioni precedenti, caratterizzato dal fatto che detto spazio

di memoria, volatile o non, è strutturato in quattro files di appoggio fittizi:

FILE1: è un BUFFER contenente la condizione originale, ovvero quella prima del "booting", di almeno una parte della RAM;

FILE2: è un'area di memoria che agisce come una RAM simulata allo scopo di far lavorare il virus in questa RAM fittizia anziché in quella vera;

FILE3: è costituito da un'altra area di memoria e simula il disco fisso in modo che il virus scriva su questo file invece che sul vero disco fisso;

FILE4: è costituito da un BUFFER atto a contenere i cambiamenti eventualmente apportati dal programma di "boot sector" al media sorgente.

3. Procedimento di cui alle rivendicazioni precedenti, caratterizzato dal fatto di comprendere le seguenti fasi:

1) bloccaggio di tutti gli INTERRUPT, affinché non ci siano interferenze durante il salvataggio della RAM convenzionale nel FILE 1;

2) salvataggio della RAM convenzionale nel FILE 1;

3) modificazione della tabella degli INTERRUPT, in

modo tale che non sia possibile far partire un programma già residente in memoria;

4) rimozione del blocco degli INTERRUPT;

5) caricamento del "boot program" del supporto di memoria non volatile sia in memoria che nel FILE2;

6) controllo della successiva istruzione da eseguire presente nel "boot program";

7) verifica della pericolosità dell'istruzione trovata nel "boot program"; se non lo è, si procede con la fase 8, altrimenti si passa alla fase 12;

8) settaggio dell'interrupt vector e del trapflag in modo che, dopo l'esecuzione dell'istruzione, il controllo torni alla procedura antivirus stessa;

9) esecuzione dell'istruzione giudicata non pericolosa;

10) cancellazione del trap flag;

11) se detta istruzione non è l'ultima si ritorna al passo n° 6, altrimenti si prosegue con il passo 13;

12) esecuzione di una serie di operazioni che fanno agire detta istruzione pericolosa sui files fittizi (FILE2÷FILE4) anziché sul vero disco fisso, poi si prosegue con la fase 11;

13) si salvano i dati forniti dal "boot program" nel FILE4;

14) si ripristina il contenuto iniziale della RAM

convenzionale tramite il FILE1;

15) nel caso in cui ci siano state operazioni pericolose si avverte l'utente della presenza di virus suggerendo di formattare il media (se è scrivibile), poi si consegnano i dati ottenuti, che si trovano nel FILE4, al sistema che può leggere il supporto di memoria non volatile;

16) si cancellano i files di lavoro e si termina la procedura antivirus.

4. Procedimento di cui alle rivendicazioni precedenti, caratterizzato dal fatto che i files di appoggio fittizzi sono costruiti nella RAM oppure sul disco fisso del PC.

5. Procedimento di cui alle rivendicazioni precedenti, caratterizzato dal fatto che le istruzioni della fase 12 verificano che, nel caso in cui venga letto un campo già scritto precedentemente dal "boot program", detta lettura avvenga sul corrispondente file fittizio.

6. Programma antivirus caratterizzato dal fatto di eseguire le fasi comprese nel procedimento di cui alle rivendicazioni precedenti.

7. Programma antivirus di cui alla rivendicazione 6, caratterizzato dal fatto di essere di tipo firmware e di essere memorizzato direttamente nel

BIOS del computer.

8. Programma antivirus di cui alle rivendicazioni da 6 in poi, caratterizzato dal fatto di essere memorizzato nella zona non riscrivibile dei BIOS.

Per il Richiedente,

il Rappresentante.

Maurizio SARPI
dello
Studio FERRARIO

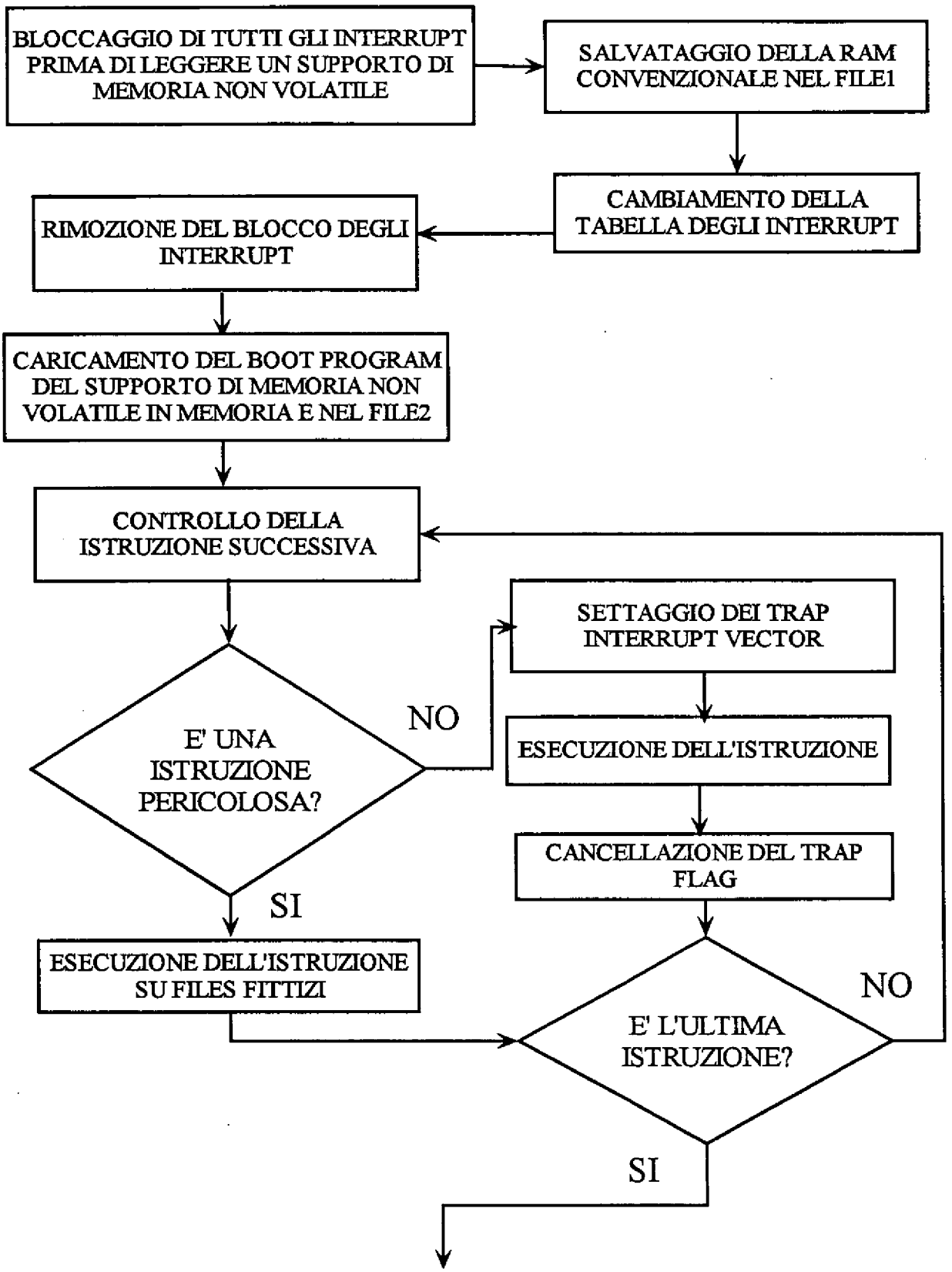

FIG. 1

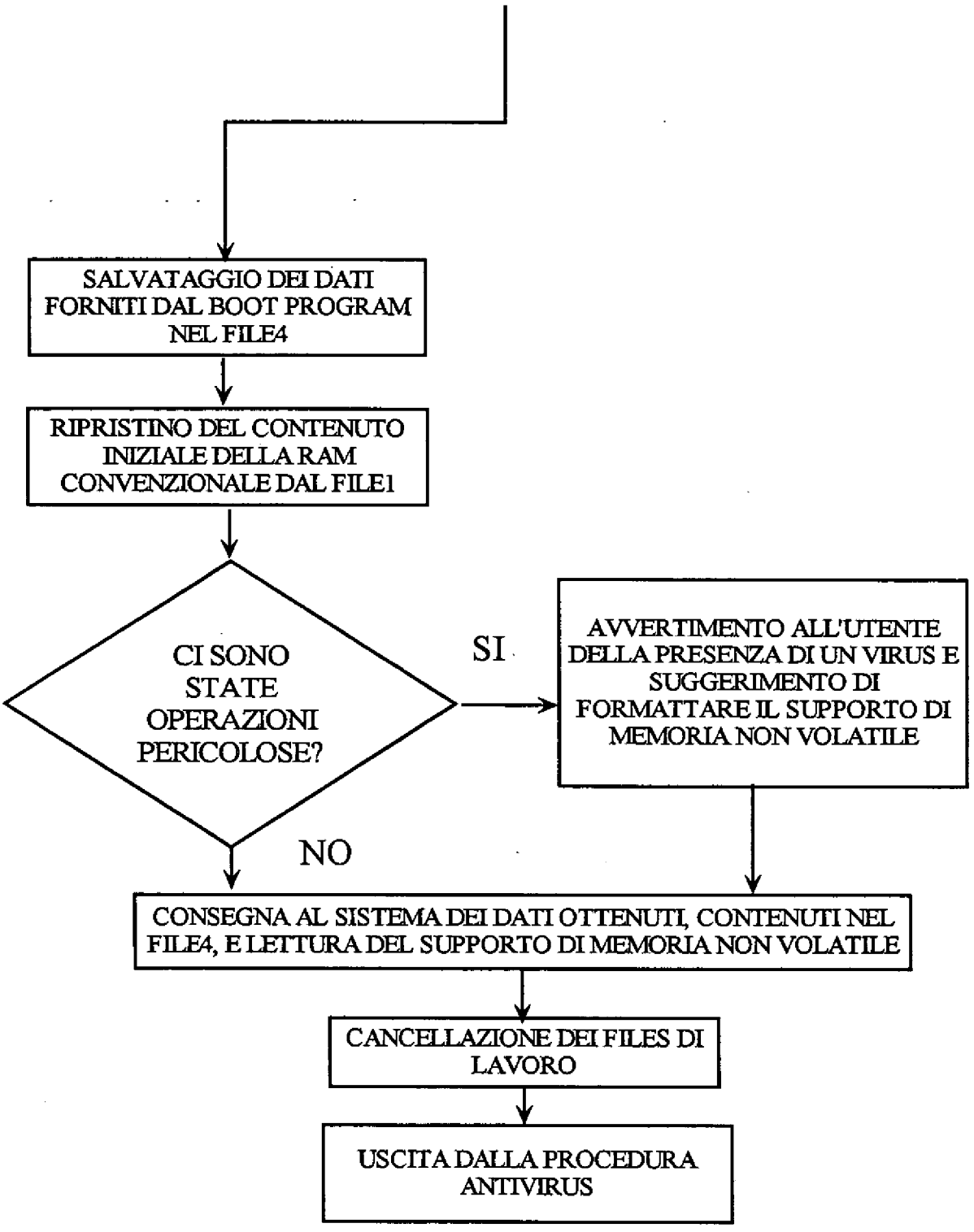

FIG. 2

Maurizio SARPI
dello
Studio FERRARIO