

Tema

Virusii calculatoarelor

1. Virusii informatici – prezentare generală
2. Istoria virusilor
3. Tipuri de virusi

1. Virușii informatici – prezentare generală

Programele daunatoare pot fi instalate chiar și manual pe o singur calculator. Ele de asemenea pot fi construite în variate pachete comerciale de soft. Ele sunt foarte greu de detectat înainte de activitățile de payload (activități pe care trebuie să le facă un program daunator).

1. Virușii informatici – prezentare generală

- **Un virus informatic** (de computer) clasic este un program proiectat să se autoreplice și să se răspândească prin rețele, memorii infectând cât mai multe computere, fără ca utilizatorii să-și dea seama de acest lucru.
- Virușii se răspîndesc atașându-se de alte programe, fișiere executabile, documente, sau unii pot să infecteze sectorul de boot al discului.
- Când se lansează în execuție un fișier infectat, se lansează și virusul în execuție.
- Adesea, virusul rămâne rezident în memoria computerului, pentru a putea infecta următorul program lansat în execuție, sau următoarea memorie accesată.
- Ceea ce face virușii periculoși este abilitatea lor de a executa acțiuni în calculator. În timp ce unele din aceste acțiuni sunt neplăcute (cum ar fi afișarea unui mesaj la o anumită dată sau ca răspuns la o anumită acțiune a utilizatorului, iar altele enervante (cum ar fi reducerea performanțelor calculatorului), există viruși care pot provoca adevărate catastrofe, distrugând fișiere de date, documente, sau făcând calculatorul inutilizabil.

Ciclul de viață al virușilor calculatoarelor

- **Crearea** – programul de tip virus este creat;
- **Replicarea** – virusul este copiat de pe un PC pe altul;
- **Activarea** – virusul declanșează acțiunea pentru care a fost creat și generează efectele distructive;
- **Descoperirea** – vir. este detectat și descris pe în documentație specială;
- **Asimilarea** – companiile care realizează soft antivirus își modifică programele lor prin includerea pe lista virușilor de îndepărtat și a acestui virus;
- **Eradicarea** – se folosește softul antivirus pentru a elimina efectele virusului.

Fazele Virusilor

- **Dormant phase:** virusul este “idle”.
- **Propagation phase:** virusul plaseaza o copie a sa in alte programe.
- **Triggering phase:** virusul este activat sa faca functia pentru care el a fost creat.
- **Execution phase:** functia este efectuata.

Simptomele unui sistem virusat

- fișierele sistem cresc în lungime;
- blocări frecvente - majoritatea virușilor sunt extrem de prost scriși și blochează calculatorul extrem de des;
- mesaje ciudate, melodii sau sunete suspecte în difuzor. Mulți viruși își fac anunțată prezența prin astfel de efecte;
- distrugerile de date sunt alt efect al virușilor. Dispariția subită a unui fișier sau erori ale sistemului de fișiere sunt clasice;
- încetinirea accesului la disc este produs de unii viruși stealth care se interpun între programe și sistemul de acces la discuri;
- la apăsarea tastelor CTRL+ALT+DEL calculatorul boot-ează instantaneu fără a mai trece prin ecranul de POST (power on, self test);
- nu mai pornește Windows sau se raportează că accesul la disc se face prin BIOS;
- schimbări ale marcajului de timp al fișierelor;
- încărcarea mai grea a programelor;
- operarea încetă a calculatorului;
- sectoare defecte pe dischete etc.

Simptomele de infectare cu Virusi

- Programele se incarca mai greu decit de obicei.
- Hard-diskul este accesat fara vreo explicatie logica.
- Mareste utilizarea spatiului de disk.
- Aparitia de caractere stranii in listele de directorii si fisiere.
- Aparitia de mesaje stranii ca “Happy birthday”, “Driver memory error”.
- Programele se pot bloca sau sa nu functioneze.

2. Istoria virușilor

- Istoria virusilor de calculatorare este lunga si interesanta care s-a dezvoltat foarte impunator odata cu dezvoltarea industriei PC.
- In anul 1986, niste programatori de la Basic&Amjad au descoperit ca un anumit sector dintr-un floppy disk contine un cod executabil care functiona de cite ori porneau computerul cu discheta montata in unitate. Acestora le-a venit ideea înlocuirii acestui cod executabil cu un program propriu. Acest program putea beneficia de memorie si putea fi astfel copiat în orice dischetă si lansat de pe orice calculator de tip PC. Ei au numit acest program virus, ocupând doar 360 KB dintr-un floppy disc.

2. Istoria virușilor

- In acelasi an programatorul Ralf Burger a descoperit ca un fisier poate fi facut sa se autocopieze, atasind o copie intr-un alt director.
- La scurt timp au inceput sa apara numerosi virusi care au evoluat rapid luind diverse forme si inglobind idei din ce in ce mai sofisticate.
- In 1990 erau cunoscuti 300 virusi
- In 1995 s-au inregistrat 7000 virusi.
- In 1995 a aparut conceptul de macrovirus. Acestia nu erau adresati numai anumitor platforme specifice, astfel ca ei puteau sa fie folositi pentru orice program, usurindu-se calea de aparitie a cunoscutilor microvirusi.

2. Istoria virusilor

- Primele programe virusulente, le-am putea numi chiar primitive, măreau dimensiunea fișierelor și reduceau viteza de răspuns, afectând performanțele computerului.
- Mulți viruși cautau doar să se răspândească, nu să afecteze computerul, astfel încât nu produceau daune în mod intenționat.
- Există posibilitatea ca virușii să interacționeze întâmplător cu alte programe sau chiar cu hardware-ul și să încetinească sau să oprească sistemul operațional.
- Virușii de ultimile generații, sunt mult mai periculoși, aceștia pot modifica sau distruge datele, sau pot șterge fișierele și pot reformata hard-discul, efectuează transferuri bănești, spionează etc.

2. Istoria virușilor

1949 John von Neumann a pus pentru prima oara bazele teoriilor legate de programele care se autoreproduc.

1950 Bell Labs au lansat *Core Wars* – lupta dintre două programe, ambele încercând să preia controlul calc.

1970 Gregory Benford a folosit termenul *virus* pentru a face referire la codurile autoreplicabile din sistemele Arpanet

1981

Virusii Apple 1, 2, și 3 sunt printre primii viruși în libertate "in the wild". Descoperit în SO Apple II, virusul a fost transmis cu numele *Elk Cloner*, dar nu a avut efect distructiv, ci afișa poezia:

**Îți ca ocupa toate discurile, Procesoarelor le va închide pliscurile, Da, îsta-i Cloner!,
Se va lipi de tine scai, Și-ți va face RAM-ul putregai, Semnează Cloner**

1983(85)

În teza sa de doctorat *Computer Viruses*, Fred Cohen definește pentru prima oară formal un virus de calculator ca fiind "un program ce poate afecta alte programe de calculator, modificându-le într-un mod care presupune abordarea unor copii evoluat ale lor."

1986

Doi programatori, Basit și Amjad, înlocuiesc codul executabil din sectorul boot al unui floppy-disk cu propriul lor cod, care infecta fiecare floppy de 360 Kb accesat pe orice drive. Floppy-urile infectate aveau "© Brain" ca eticheta de disc (volum label).

1988

Scapa din lesa unul dintre cei mai cunoscuți viruși: *Jerusalem*. Activat în fiecare vineri 13, virusul afectează fișierele .exe și .com și șterge toate programele rulate în cursul acelei zile.

1990

Symantec lansează pe piața Norton AntiVirus, unul dintre primele programe antivirus dezvoltate de către una dintre marile companii.

1991

Tequila este primul virus polimorf cu răspândire pe scară largă găsit "in the wild". Virușii polimorfi fac ca detectarea lor de către scanerul de viruși să fie dificilă, prin schimbarea modului de acțiune cu fiecare nouă infecție.

2. Istoria virușilor

1992 Apogeul Virusologiei - exista 1300 de virusi, cu aproape 420% mai multi decat in decembrie 1990. Previziunile sumbre ale virusului *Michelangelo* ameninta harddiskurile a circa 5 milioane de calculatoare pe data de 6 martie. In realitate, au fost mai putine...

1994

Farsa de proportii din partea email-ului hoax (alarma falsa)*Good Times*. Farsa se bazeaza pe amenintarea unui virus sofisticat care e capabil sa stearga un intreg hard prin simpla deschidere a emailului al carui subiect este "Good Times". Desi se stie despre ce e vorba, hoaxul revine la un interval de 6-12 luni.

1995

Word Concept, virus de Microsoft Word, devine unul dintre cei mai raspanditi virusi din anii '90.

1998

StrangeBrew, actualmente inofensiv si totusi raportat, este primul virus care infecteaza fisierele Java. Virusul modifica fisierele CLASS adaugand la mijlocul acestora o copie a sa si incepand executarea programului din interiorul sectiunii virusate.

Virusul *Cernobal* se raspandeste rapid prin intermediul fisierele ".exe". Dupa cum o sugereaza si notorietatea numelui sau, virusul este nemilos, atacand nu numai fisierele dar si un anumit cip din interiorul computerelor infectate.

1999

Virusul *Melissa* executa un macro dintr-un document atasat emailului, care transmite mai departe documentul la 50 de adrese existente in Outlook address book. Virusul infecteaza si documente Word pe care le trimite ca atasamente.

Melissa -1 milion de calculatoare.

Bubble Boy este primul virus care nu mai depinde de deschiderea atasamentului pentru a se executa. De indata ce userul deschide email-ul, Bubble Boy se si pune pe treaba.

2000

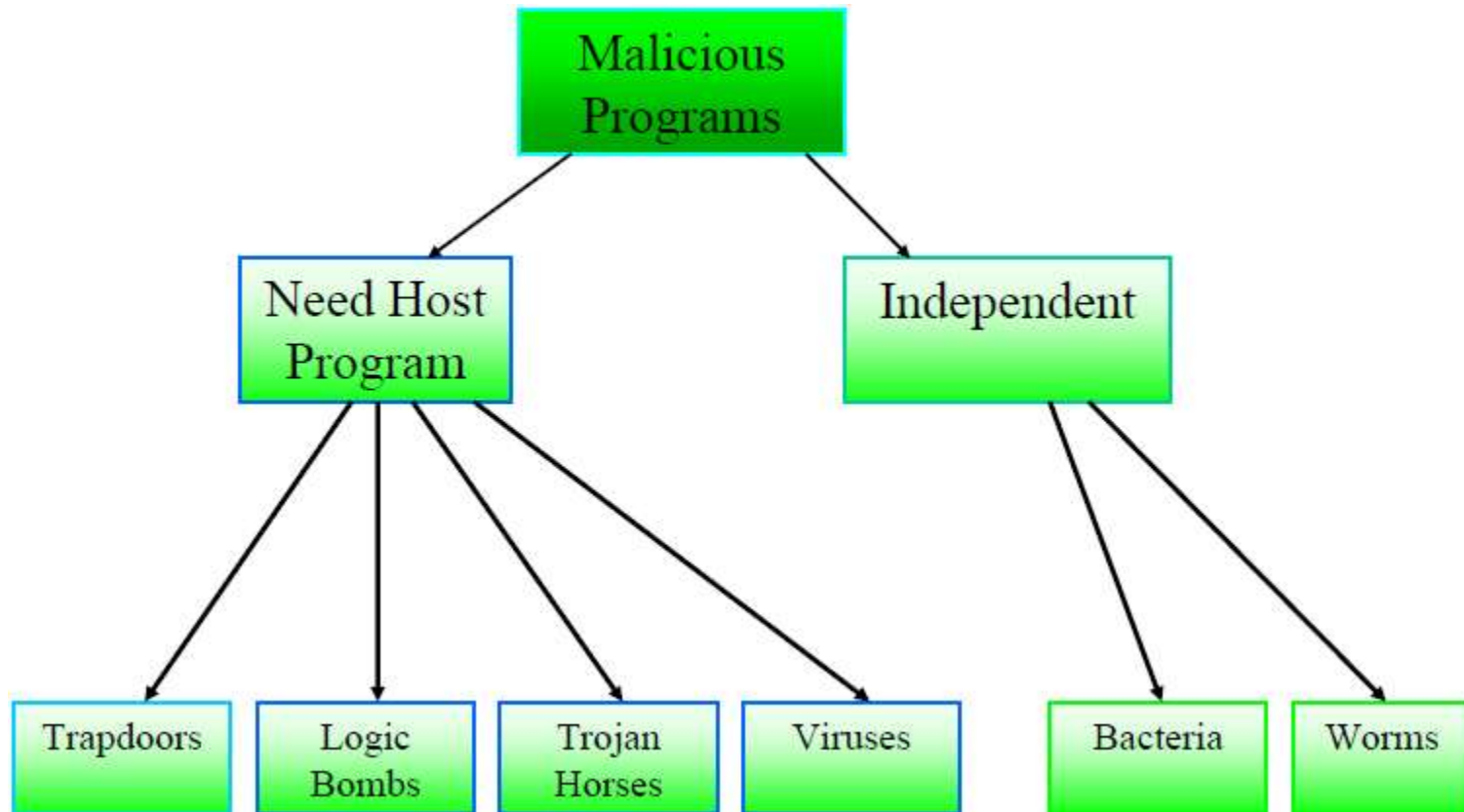
Love Bug, cunoscut si sub numele de *ILOVEYOU* se raspandeste via Outlook, asemanator modului de raspandire al Melissei. Acest virus e primit ca un atasament .

2001 – vedetele anului au fost Nimda, CodeRed, Aliz / au fost adevarati pioneri în stabilirea viitoarelor tendinte de securitate. Canalele ICQ si MS Messenger au fost pentru prima dată folosite ca căi de transmitere a virușilor. Virușii pentru **Linux**. Primul virus RedHat Linux a intrat fraudulos in rețelele NASA... Au apărut **viermii** – invizibili care infectat fara a folosi fisiere, existau numai in RAM și se răspîndeau ca pachete de date special configurate.

2004 Primii viruși destinați telefoanelor mobile: Cabir, Mosquitos...

2005 s-a dezvoltat phishing-ul, troieni spioni...Virușii și viermii au devenit mai moderni*Sober.P* – mesaje legate de deschiderea caselor de bilete la Campionatul Mondial de fotbal, infectind calc. din 40 de țări.

Taxonomia programelor daunatoare.



Definitii

- **Trapdoor:** puncte de intrare alternative scrise in coduri de depanare care pot permite utilizatorilor nedoriti accesul catre sistem.
- **Logic Boombs:** un cod daunator care se activeaza la un anumit timp (ex: data, ora...)
- **Trojan Horse:** instructiuni dintr-un program care cauzeaza lucruri rele ca sa se intimple(ex: trimiterea de date sau parole la o alta persoana prin internet.)
- **Virusi:** cod care se copie in alte programe.
- **Bacteria:** un program care se reproduce pina umple spatiul de disk, sau pina incarca CPU.
- **Worm:** program care se copie pe sine in retea.(de obicei atasate de mesajele de pe email sau documentelor atasate.)

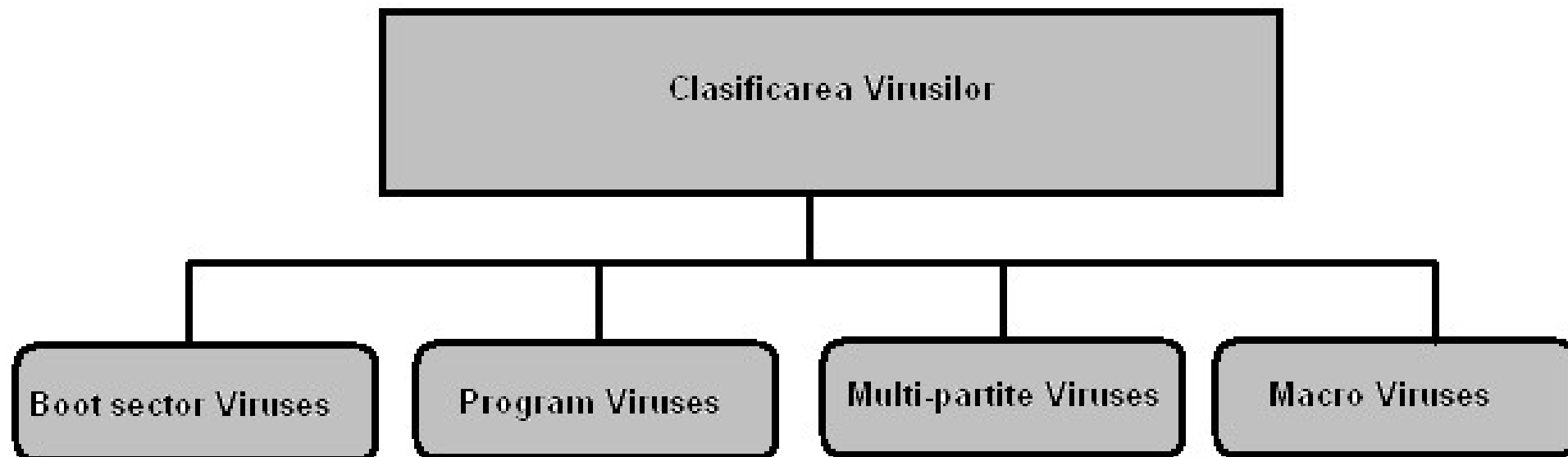
Ce este un virus de calculator?

- Un **virus de calculator** este un program de dimensiuni mici, construit cu scopul de a face o gluma sau de a sabota pe cineva. Acest program are proprietatea ca se autoreproduce, atasandu-se altor programe si executind operatii nedorite sau de distrugere.
- Virusul este caracterizat de urmatoarele proprietati:
 - Poate modifica fisiere si programe ale utilizatorilor, prin inserarea in acestea a intregului cod sau numai a unei parti speciale din codul sau.
 - Modificarile pot fi provocate nu numai programelor ci si unor grupuri de programe
 - Are nevoie si poate sa recunoasca daca un program a fost deja infectat pentru a interzice o noua modificare.

Structura virusilor

- **Replicator** – functia sa consta in asigurarea supravietuirii virusului pe un sistem. Majoritatea virusilor de succes fac acest lucru fara a provoca daune asupra sistemului. De fiecare data cind programul este rulat virusul se “trezeste” si va incepe sa se reproduca.
- **Concealed** – aceasta parte a virusului are functionalitatea de a ascunde prezenta virusului prin metode diferite si de a executa scopul sau.

Clasificarea Virusilor



Boot Sector Viruses

- acesti virusi infecteaza sectoarele de boot ale hard disk-lui.
- Ei inlocuiesc programul de boot (care este responsabil de incarcarea SO in memorie) copiind-ul in alta parte sau rescriind-ul.
- Ei se incarca in memorie daca calculatorul incearca sa citeasca diskul in timp ce are loc bootarea.

Clasificarea Virusilor

- **Program Viruses**
 - acești viruși infectează fișierele de program cu așa extensii ca: .BIN, .COM, .EXE, .DRV și .SYS.
 - Acești viruși se încarcă în memorie în momentul execuției programelor.
 - Virusul devine activ în memorie copiindu-se pe sine și infectând fișierele de pe disk.
- **Multi partite Viruses**
 - reprezintă un hibrid de viruși program și viruși de boot.
 - Ei infectează fișierele de program și când programele infectate sunt executate acești viruși infectează sectoarele de boot.
 - Următoarea dată când încarcăm calculatorul virusul se încarcă în memorie și infectează alte fișiere program.

Clasificarea Virusilor

- **Macro Viruses**
 - reprezinta noi tipuri de virusi care infecteaza macrourele intr-un document sau template.
 - Cind deschidem un document Word sau de tip spreadsheet, virusul macro este activat si el infecteaza template-urile normale si fisiere a caror scop principal este de a stoca setarile de formatare a documentului.
 - Fiecare document pe care-l deschidem si se refera la un template normal, prin urmare devine infectat cu un virus macro.
 - Din momentul in care acest virus se ataseaza la documente, infectia se poate raspindii in cazul in care astfel de documente sunt deschise de pe alte computere.

3. Tipuri de viruși

1. Virușii fișierelor infestate sau virușii programelor – infectează fișiere, dar modul de lucru este diferit de la un virus la altul:

- virușii paraziti, schimbă conținutul fișierelor incit sa devina total sau partial utilizabile (se strecoară la inceput, mijloc sau sf. fisierului)
- virușii suprascrierii – inclocuiește codul programului cu propriul cod / distruge pr.
- Virușii punctelor de intrare obscure –cod scurt in fișier...
- Virușii companion – clonează fișierele și le execută pe cele clonate...
- Viermii - copie codul intr-un fișier nou
- Virușii legăturănu schimbă codul fișierului, ci SO este obligat...

3. Tipuri de viruși

2. Virușii sectoarelor de boot – infectează sectoarele boot ale hard , este declansat la prima incercare de initializare a sistemului. Au ca obiectiv distrugerea sau suprascrierea sectoarelor de boot sau a datelor de pe hard

3. Tipuri de viruși

3. Virușii macro – sunt lansati cind se deschide un document infectat (macrou-urile autorun ale unei aplicatii)

3. Tipuri de viruși

4. Virușii de tip script – scrise in limbaje script (Java script, ActiveX) care folosesc funcția gazdă a Windows Scripting Host din Microsoft Windows pentru a se autoactiva, ceea ce permite virusilor sa infecteze si alte fisiere din aceasta clasa



3. Tipuri de viruși

6. Viermii –se autocopieaza de la un PC la altul, fara actiunea utilizatorului, apeleaza la mesajele e-mail, canalele Internet, mesageria rapidă...Cei mai periculoși sunt viermii rețelelor – care exploateaza partile nepazite ale serverelor si browser-elor...



3. Tipuri de viruși

5. Caii troieni – nu se pot autoreplica (cum sunt și backdoors, rootkits), patrund prin înșelătorie:

- atasare la e-mail
- Crearea de fișiere foarte atractive
- Ascunderea tipului real al fișierului

backdoors

- Troienii ușilor din spate – PC unei rețele este controlat de alt PC de la distanță printr-un utilitar de administrare a rețelelor
- Port-sacner pentru IP

Rootkit

- Termenul **rootkit** face referire la acel cod software utilizat pentru modificarea sau simularea funcțiilor de bază ale unui sistem de operare, dând posibilitatea unui atacator să acceseze un sistem informatic de la distanță. Un rootkit poate, de exemplu, să fie disimulat în comanda dir (windows) sau ls (unix), astfel încât pe lângă funcția de bază a acelei comenzi să realizeze și alte acțiuni despre care utilizatorul nu este conștient .

Rootkit sunt împărțite în două categorii:

- user – mode – modifică cod software din sistemul de operare folosit la nivel utilizator (dir, ch, ls);
- kernel – mode – modifică cod software din sistemul de operare utilizat la nivel nucleu (kernel) - servicii, daemons, procese și fire de execuție, management întreruperi – etc.

Detecția rootkit-ului de nivel kernel este foarte dificilă, deoarece programele antimalware sunt instalate și funcționează la nivel utilizator.

Adware

- **Adware** este orice program care afișează reclame la rulare, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up (care deschide ferestre noi cu reclame, deasupra tuturor ferestrelor). Unele programe adware pot fi considerate o formă de [spyware](#) care nu colectează date de marketing, ci doar transmit reclame.

spyware

- ***Programele-spioni*** destul de capabile, sunt în stare să urmărească acțiunile utilizatorului la computer sau în rețeaua globală pentru ca apoi aceste informații să fie expediate pe adrese anumite. Așa aplicații-spioni sunt și în mediul ultimilor jocuri computaționale. Ca simplu exemplu clasic poate servi exemplul cu dl Simeon Garfinkel, specialist-expert în domeniul Securității Informaționale din SUA. Aflându-se în avion, deasupra Atlanticului, ca de obicei lucra la notebookul său, la un anumit timp a observat că computerul a trecut de la sine în regimul on-line. Readucând computerul în regimul off-line a prelungit introducerea textului. La câteva minute computerul iarăși a ieșit de sub controlul utilizatorului trecând în regimul de expediere a mesajelor electronice. Interesul și profesionalismul l-a făcut pe S. Garfinkel să se ocupe de acest caz, depistând în rezultat un program-spion implantat DSSAgent, care putea fi oprit numai prin opțiunile panoului de dirijare. Cercetările adăugătoare au demonstrat modificarea Registrului de sistem al SO în așa mod că această aplicație se lansa odată cu conectarea computerului. Pe HDD această aplicație-spion s-a mascat sub formă de fișier de sistem în mapa: Windows\Sistem,

Metode de apărare cu rol preventiv

- Evitarea schimbului de programe și suporturi de memorii între utilizatori, care au fost obținute de la necunoscuți, prieteni sau de la întreprinderi neautorizate în comercializarea de produse informatice.
- Numai softul obținut de la surse cunoscute pot fi introduse în calculator (chiar și cele mai bune programe realizate de programatorii unei firme trebuie observate cu mare atenție).
- Se folosesc bariere fizice sau logice acolo unde este posibil, precum firewall, comutatoare de protecție la scriere pe discuri etc.
- Stabilirea unor politici sau standarde de control al programelor și respectarea lor.

Cum sa protejam calculatorul impotriva virusilor ?

- Pentru a proteja calculatorul impotriva virusilor urmati urmatorii pasi:
 - Porniti firewall-ul calculatorului.
 - Mentineti sistemul de operare in stare actualizata.
 - Utilizati un antivirus cu baza de date actualizata.
 - Utilizati un soft antispyware.

Evitarea detectării

- “last modified” date
- Cyclic redundancy checks
- infect files without increasing their sizes or damaging the files (*cavity viruses*)
- kill the tasks associated with antivirus
- Avoiding bait files