VIRUSI. PROGRAME ANTIVIRUS

Virusii informatici – sunt, in esenta,microprograme greu de depistat,ascunse in alte programe,care asteapta un moment favorabil pentru a provoca defectiuni ale sistemului de calcul(blocarea acestuia,comenzi sau mesaje neasteptate,alte actiuni distructive).

Se poate aprecia ca un virus informatic este un microprogram cu actiune distructiva localizat in principal in memoria interna,unde astepta un semnal pentru a-si declansa activitatea.

O clasificare riguroasa nu exista inca,dar se poate face tinand seama de anumite criterii. In forma cea mai generala virusii se impart in:

- Virusi hardware
- Virusi software

Virusii hardware sunt mai rar intalniti,acestia fiind de regula, livrati o data cu echipamentul. Majoritatea sunt virusi software,creati de specialisti in informatica foarte abili si buni cunoscatoari ai sistemelor de calcul,in special al modului cum lucreaza software-ul de baza si cel aplicativ.

Din punct de vedere al capacitatii de multiplicare,virusii se impart in doua categorii:

- Virusi care se reproduc,infecteaza si distrug
- Virusi care nu se reproduc,dar se infiltreaza in sistem si provoaca distrugeri lente,fara sa lase urme(Worms).

In functie de tipul distrugerilor in sistem se disting:

- Virusi care provoaca distrugerea programului in care sunt inclusi
- Virusi care nu provoaca distrugeri,dar incomedeaza lucrul cu sistemul de calcul; se manifesta prin incetinirea vitezei de lucru,blocarea tastaturii,reinitializarea aleatorie a sistemului, afisarea unor mesaje sau imagini nejustificate
- Virusi cu mare putere de distrugere,care provoaca incideante pentru intreg sistemul, cum ar fi: distrugerea tabelei de alocare a fisierelor de pe hard disk, modificarea continutului directorului radacina,alterarea integrala si irecuperabila a informatiei existente

Primii virusi atacau programele gazda. De exemplu, “Brain” inlocuia numele volumului dischetei cu al sau; “Vendredi 13” crestea dimensiunea programelor cu 512 octetil “Data crime” si “Vienna” se semnau prin respectiv 1168 si 648 octeti.

Primele programe antivirus puteau repera usor acesti invadatori. Creatorii de virusi au reactionat insa prin adoptarea unor strategii mai performante si au dezvoltat proceduri capabile sa infecteze un program,fara ca alterarea sa fie prea ostentativa.

Odata introdus pe disc,a doua faza a vietii unui virus este autoprogramarea. Virusii incearca sa infecteze cat mai multe programe,inainte de a ataca propriu-zis. Pentru a opera cat mai eficient, virusii isi lasa semnatur in fiecare program infectat,pentru a nu-l contamina inca o data. Pe acest principiu lucreaza si antivirusii,adica pe reperarea unei intruziuni. Ei analizeaza unitatiile de disc pentru a cauta semnaturile cunoscute. Aceasta tehnica prezinta insa un defect major: virusul trebuie indentificat,deci tabela de senaturi trebuie permanent reactualizata.

Virusii au forme de manifestare cat se poate de diverse.Unii se multumesc sa afiseze mesaje de pace sau sa cante o melodie. Altii perturba lucrul utilizatorului,insa fara

consecinte prea dramatice. De exemplu.” KeyPress” duce la aparitia pe ecran a sirului “AAAAA”,daca se apasa tasta “A”. Cei mai neplacuti virusi sunt aceia care sunt programati pentru distrugerea datelor: stergeri,formatari de disc, bruiaj de informatii, modificari in bazele de date,etc.

Uneori,virusii atacau dupa o lunga perioada de somnolenta. De exemplu,” Golden Gate” nu devine agresiv decat dupa ce a infectat 500 de programe, “Cyber TechB” nu a actionat, in schimb, decat pana la 31 decembrie 1993.

Morala: utilizatorul avizat(si patit) trebuie sa aiba grija ca periodic sa ruleze programe antivitus.

In manualul de utilizare al MS-DOS,Microsoft imparte virusii in trei categorii:

- Virusi care infecteaza sistemul de boot
- Virusi care infecteaza fisierele
- Virusi Cal Troian

Ultimii sunt acele programe care aparent au oa numita intrebuintare,dar sunt inzestrati cu proceduri secundare distructive. Totusi, o clasificare mai amanuntita a virusilor ar arata astfel:

- Armati – o forma mai recenta de virusi,care contin proceduri ce impiedica dezasamblarea si analiza de catre un antivirus, editorii fiind nevoiti sa-si dubleze eforturile pentru a dezvolta antidotul (ex:” Whale”)
- Autoencriptori – inglobeaza in corpul lor metode de criptare sofisticate facand detectia destul de dificila. Din fericire, pot fi descoperiti prin faptul ca incorporeaza o rutina de decriptare(ex: “Cascade”)
- Camarazi – sunt avantajati de o particularitate a DOS-ului, care executa programele .com inaintea celor .exe. Acesti virusi se ataseaza de fisierele .exe,apoi le copiaza schimband extensia in .com. Fisierul original nu se modifica si poate trece de testul antivirusilor avansati. Odata lansat in executie fisierul respectiv,ceea ce se execua nu este fisierul .com, ci fisierul .exe infectat. Acest lucru determina propagarea virusilor si la alte aplicatii
- Furisati(stealth) – acesti virusi isi mascheaza prezenta prin deturnarea intreruperilor DOS. Astfel, comanda dir nu permite observarea faptului ca dimensiunea unui fisier executabil a crescut,deci este infectat . Exemplu:“512”,”Atheus”,”Brain”, ”Damage”, ”Gremlin”,”Holocaust”,”Telecom”
- Infectie multipla – cu cativa ani in urma virusi erau repartizati in doua grupuri bine separate: cei care infectau programele si cei care operau asupra sectorului de boot si a tebelelor de partitii. Virusii cu infectie multipla,mai rcenti, pot contamina ambele tipuri de elemente. Exemplu: ”Authax”,” Crazy Eddie”,”Invader”,” Malaga”,etc
- Polimorfi –sunt cei mai sofisticati dintre cei intalniti pana acum. Un “motor” de mutatii permite transformarea lor in mii de variante de cod diferite. Exemplu: ”Andre”,” Cheeba”,”Dark Avenger”,”Phoenix 2000”,” Maltese Fish”,etc
- Virusi ai sectorului de boot si ai tabelelor de partitii –ei infecteaza una si/sau cealalta dintre aceste zone critice ale dischetei sau hard disk-ului. Infectarea sectorului de boot este periculoasa,deoarece la pornirea calculatorului codul special MBP(Master Boot Program) de pe discheta se executata inainte de DOS. Daca acolo este prezent un virus, s-ar putea sa nu fie reperabil. Tabelele de partitii contin informatii despre organizare structurii discului,ele neputand fi contaminate,ci doar stricate. Majoritatea antivirusilor actuali pot detecta o infectie in MBP,propund,in general, suprimarea

MBP-ului si inlocuirea lui cu o forma sanatoasa(de exemplu cum procedeaza Norton Antivirus). Exemplu:” Alameda”,”Ashar”,”Bloodie”,”Cannabis”,”Chaos”.

Modul de infectare

Mecanismul de contaminare clasic consta in ramanerea rezidenta in memoria interna a secventei purtatoare a virusului, ascunsa intr-un program care se executa. Programul modificat prin actiunea virusului,cu secventa de virus incorporata,este salvat pe discul care a fost lansat, constituind la randul sau un nou purtator de virus. Virusarea este relativ rapida, avand ca efect infectarea tuturor programelo lansate in executie,atata timp cat virusul este rezident in memoria interna.

O tehnica mai evoluata de contaminare consta in introducerea secventei de program ce contine virusul,in urma procesului de instalare a unui produs; in momentul instalarii produsului,acestuia i se a adauga instructiuni intr-o secventa ce defineste un cod de virus.

Cele mai vulnerabile fisiere sunt fisierele executabile de tip .exe si .com, deoarece acestea contin programele in forma executabila, care se incarca in memoria interna pentru executie,unde se localizeaza initial virusul; de asemenea, pentru a patrunde in zonele protejate ale sistemului, virusul are nevoie de drepturi de acces pe care nu la are, in timp ce programul pe care s-a implantat ii mai gireaza aceste drepturi,fara ca utilizatorul sa aiba cunostiita de acest lucru.

Modalitati de protectie. Programe antivirus

Odata ajuns in calculator,pentru a-si indeplini in mod eficient scopul,virusul actioneaza in doua etape. In prima faza de multiplicare,virusul se reproduce doar,marind astfel considerabil potentialul pentru infectari ulterioare. Din exterior nu se observa nici o activitate evidenta. O parte a codului de virus testeaza constant daca au fost indeplinite conditiile de declansare(rularea de un numar de ori a unui program,atingerea unei anumite date de catre ceasul sistemului vineri 13 sau 1 aprilie sunt alegeri obisnuite, etc). Urmatoarea faza este cea activa,usor de recunoscut dupa actiunile sale tipice: modificarea imaginii de pe ecran,stergerea unor fisiere sau chiar reformatatrea hard disk-ului.

Pe langa fisierele executabile sunt atacate si datele de baza. Desii virusii au nevoie de o gazda pentru a putea supravietui,modul de coexistenta cu ea este diferit de la un virus la altul. Exista virusi paraziti care nu altereaza codul gazdei,ci doar se atasaza. Atasarea se poate face la inceputul, la sfarsitul sau la mijlocul codului gazda, ca o subrutina proprie.

In contrast cu acetia, altii se inscriu pur si simplu pe o parte din codul gazdei. Acestia sunt deosebit de periculosi, deoarece fisierul gazda este imposibil de recuperat.

Pentru ca virusul sa se extinda, codul sau trebuie executat fie ca urmare indirecta a invocarii de catre utilizator a unui program infectat, fie direct, ca facand parte din secventa de initializare.

O speranta in diminuarea pericolului virusilor o constituie realizarea noilor tipuri de programe cu protectii incluse. Una dintre acestea consta in includerea in program a unei sume de control care verifica la lansare si blocheaza sistemul daca este infectat. In perspectiva,se pot folosi sisteme de operare mai putin vulnerabile. Un astfel de sistem

de oprerare este UNIX,in care programul utilizator care poate fi infectat nu are acces la toate resursele sistemului.

Virusii care se inmultesc din ce in ce mai mult, polifereaza datorita urmatorilor factori:

Comment [s1]:

- Punerea in circulatie prin retele internationale a unei colectii de programe sursa de virusi, pe baza carora s-au scris mai multe variante de noi virusi
- Aparitia si punerea in circulatie, cu documentatie sursa completa, a unor pachete de programe specializate pentru generarea de virusi. Doua dintre acestea sunt Man's VCL (Nuke) si PC-MPC de la Phalcon/Skim; ambele au fost puse in circulatie in 1992.
- Distribuirea in 1992, via BBS-ului bulgar, a programului MTE - " masina de produs mutatii"- conceput de Dark Avenger din Sofia. Acest program este insotit de o documentatie de utilizare suficient de detaliata si de un virus simplu, didactic. Link-editarea unui virus existent cu MTE si un generator de numere aleatoare duce la transformarea lui intr-un virus polimorf. Virusul polimorf are capaciatetea de a-si schimba secventa de instructiuni la fiecare multiplicare, functia de baza ramanand nealterata,dar devenind practic de nedectat prin scanare
- Raspandirea BBS-urilor (Bulletin Board System),care permit oricarui utilizator Pc dotat cu un modem sa transmita programe spre si dinspre un calculator. Un sitem este lipsit de virusi,daca in memorie nu este rezident sau ascuns nici un virus,iar programele care se ruleaza sunt curate. In aceasta conceptie, programul antivirus vizeaza atat memoria calculatoarelor, cat si programele executabile. Cum in practica nu poate fi evitata importarea de fisiere virusate,metode antivirus cauta sa asigure protectie in anumite cazuri perticulare,si anume:
    - la un prim contact cu un program,in care se recunoaste semnatura virusului, se foloseste scanarea. Aceasta consta in cautarea in cadrul programelor a unor secvente sau semnaturi caracateristice virusilor din biblioteca programului de scanare;
    - daca programele sunt deja cunoscute, nefiind la primul contact, se folosesc sume de control. Aceste sume constituie o semnatura a programului si orice modificare a lui va duce la o modificare a sumei sale de control;
    - in calculator exista o serie de programe care nu se modifica, reprezentand zestrea se soft a calculatorului, care se protejeaza pur si simplu la scriere.

Scanarea se aplica preventiv la prelucrarea fisierelor din afara sistemului,deci este utila in faza primara de raspandire a virusilor. Ea poate fi salvatoare, chiar daca se aplica ulterior (de pe o discheta sistem curata), in faza activa,deoarece in numeroase cazuri poate recupera fisierele infectate.

Concluzii:

- aria de actiune; memoria si fisierele de interes;
- protectia se mnifesta la primul contact cu orice fisier;
- permite dezinfectarea;
- nu detecteaza virusi noi. Orice virus nou trebuie introdus in lista de virusi a programului de scanare;

- timpul de scanare creste odata cu cresterea numarului de virusi cautati si cu numarul de fisiere protejate;
- exista alarme false, daca semnatura virusului este prea scurta;
- foloseste ca resursa memoria calculatorului;
- opereaza automat (ca un TSR).

Sumele de control sunt calculate cu polinoame CRC si pot detecta orice schimbare in program,chiar daca aceasta consta numai in schimbarea ordinii octetilor. Aceasta permite blocarea lansarii in executie a programelor infectate,chiar de virusi necunoscuti, dar nu permite recuperarea acestora. Metoda este deosebit de utila in faza de raspandire a virusilor,orice fisier infectat putand fi detectat. In faza activa,insa metoda este neputicioasa.

Programele de protectie –programe antivirus- au rolul de a realiza simultan urmatoarele activitati:

- prevenirea contaminarii;
- detectarea virusului;
- eliminarea virusului, cu refacerea contextului initial;

In general, exista doua categorii de programe antivirus:

- programe care verifica fisierele pentru a descoperi texte neadecvate sau sematuri de virusi recunoscuti;
- programe rezidente in memoria interna, care intercepteaza instructiunile speciale sau cele care par dubioase.

In categoria programelor de vierificare se include cele de tip SCANxxx,unde prin xxx s-a specificat numarul asociat unei versiuni, de exemplu: SCAN86, SCAN102, SCAN108, SCAN200.

Aceste programe verifica intai memoria interna si apoi unitatea de disc specifica, afisand pe monitor eventuali virusi depistati si recunoscuti in versiunea respectiva. Dupa aceasta verificare, utilizatorul va incerca aliminarea virusului depistat,prin intermediul programelor CLEARxxx, prin specificarea numelui virusului; de remarcat ca, folosind acest program, nu exista certitudinea curatirii virusilor,datorita fie a nerecunoasterii acestora, fie a localizarii acestora in locuri care nu pot fi intotdeauna reperate.