# Viruşii

- Ce este un virus de calculator?

Un virus de calculator este de obicei un program proiectat să se autoreplice şi să se împrăştie, infectând cât mai multe calculatoare, fără ca utilizatorii să îşi dea seama de acest lucru. Viruşii se imprăştie ataşându-se de alte programe, fisiere EXE sau COM, iar mai recent, si documentelor WORD, EXCEL, chiar si fisierelor HLP, sau unii pot să infecteze sectorul de boot al discului. Când se lansează în execuţie un fişier infectat, sau când se porneşte calculatorul de pe un disc sau o dischetă virusată, se lansează şi virusul in execuţie. Adesea, virusul rămâne rezident în memoria calculatorului, pentru a putea infecta următorul program lansat în execuţie, sau următoarea dischetă accesată.

Ceea ce fac viruşii periculoşi este abilitatea lor de a executa acţiuni în calculator. În timp ce unele din aceste acţiuni sunt sâcâitoare (cum ar fi afişarea unui mesaj la o anumită dată sau ca răspuns la o anumită acţiune a utilizatorului calculatorului) iar altele enervante (cum ar fi reducerea performanţelor calculatorului), există viruşi care pot provoca adevărate catastrofe, distrugând fisiere de date, documente, sau făcând calculatorul inutilizabil.

Primii viruşi au apărut acum câteva decenii, însă nu au cunoscut o răspândire la scară mondială decât după aparitia primelor PC-uri. În 1981 firma IBM scotea pe piată, alături de gigantele mainframe-uri care îi aduseseră succesul, un calculator "personal" bazat pe noul (pe atunci) procesor produs de firma Intel, 8088. Preţul acestuia era extrem de ridicat, însă produsul a fost un succes. Ca sistem de operare IBM a cumpărat MS-DOS de la firma Microsoft, care la rândul ei l-a scris pe baza sistemului de operare CP/M. Primele versiuni de DOS erau extrem de compacte (numai câteva zeci de Kb) şi nu aveau nici un protocol de securitate inclus.

Trec 5 ani si ajungem în 1986 când apăreau primele rapoarte publice indicând entităţi virale pe IBM-PC. Era vorba de virusul Brain, un virus de boot. Apar astfel programe de tip antivirus create pentru a elimina viruşii informatici. Dacă primele programe antivirus erau extrem de simple, ca si viruşii de pe atunci, programele din ziua de astăzi sunt adevărate "capodopere" de algoritmi si cod.

- ## Cum se răspândesc viruşii?

Viruşii pot proveni dintr-o varietate de surse. Pentru că un virus reprezintă cod executabil, el poate fi transmis pe toate căile normale de transmitere a informaţiei între calculatoare:
Într-un studiu din 1991 al companiei Dataquest realizat la cererea National Computer Security Association din Statele Unite, cel mai des viruşii se transmiteau prin dischete infectate (87 %). 43% din dischetele infectate, responsabile pentru introducerea viruşilor pe calculatoarele întreprinderilor erau dischete aduse de acasă. Aproape trei sferturi (71%) din infecţii au apărut în întreprinderi cu reţele de calculatoare, crescând pagubele prin rapida împrăştiere a viruşilor în toată reţeaua. În mediile de reţea, riscul infectării cu viruşi este mult crescut. Şapte la sută (7%) din viruşi proveneau din fişiere preluate de pe diverse BBS-uri (la acea dată reţeaua Internet nu avea răspândirea actuală). Alte surse de dischete infectate erau dischetele demo sau conţinând software arhivat – circa 6% din infecţiile raportate.

- ## Ce pot face viruşii?

Aşa cum am spus şi mai devreme, unii viruşi sunt enervanţi, iar alţii pot fi deosebit de periculoşi. În cazul cel mai fericit, viruşii cresc dimensiunea fişierelor şi reduc viteza de răspuns, afectând performanţele calculatorului dumneavoastră. Mulţi viruşi caută doar să se răspândească, nu să afecteze calculatorul, astfel încât nu produc daune în mod intenţionat. Totuşi, există posibilitatea ca si viruşi benigni să interacţioneze întâmplător cu alte programe sau chiar cu hardware-ul şi să încetinească sau să oprească sistemul. Alti viruşi sunt mult mai periculoşi. Aceştia pot modifica sau distruge datele, sau pot şterge fişierele şi pot reformata hard-discul.

- ## Care sunt simptomele unui sistem virusat?

Cei care sunt iniţiaţi în domeniul viruşilor de calculatoare nu vor avea probabil dificultăti în a spune dacă un calculator este suspect de a fi infectat cu un virus nou. Viruşii se pot răspândi nestingheriţi doar atâta timp cât rămân nedetectaţi. Din acest motiv, majoritatea viruşilor nu îşi manifestă prezenţa în sistem. Numai programele antivirus pot detecta prezenta unei asemenea infecţii. Există, totuşi, mai multi viruşi, ce îsi fac simţită prezenţa în sistem prin efectele secundare generate.

Câteva "simptome" specifice calculatoarelor virusate (lista este orientativă, cazurile reale fiind mult mai numeroase si diverse):

- fişierele sistem cresc în lungime (de exemplu în DOS 6.20 fişierul command.com are 54619 octeţi, iar pe un calculator virusat el poate avea, să zicem cu 1200 de octeţi mai mult, respectiv 55819);
- blocări frecvente - majoritatea viruşilor sunt extrem de prost scrişi si blochează calculatorul extrem de des. Viruşii sunt de altfel cunoscuţi ca cele mai incompatibile programe (exceptând viruşii multiplatformã, ca de exemplu clasa "Concept" - viruşii de .doc Word);
- mesaje ciudate, melodii sau sunete suspecte în difuzor. Mulţi viruţi îşi fac anunţatã prezenţa prin astfel de efecte;
- distrugerile de date sunt alt efect al viruşilor. Dispariţia subită a unui fişier sau erori ale sistemului de fişiere sunt clasice;
- încetinirea accesului la disc este produs de unii viruşi stealth care se interpun între programe şi 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);
- la comanda chkdsk majoritatea programelor executabile sunt raportate ca având o lungime incorectă: efect al unor viruşi stealth;
- dimensiunea memoriei afişată de programele specializate este mai mică decât 640Kb. Uneori acest efect este generat de unele managere de memorie fără a fi vorba de un virus, dar de obicei indică prezenţa unui virus;
- programele de tip self-check raportează cã au fost modificate;
- nu mai porneşte Windows sau se raportează că accesul la disc se face prin BIOS;
- schimbări ale marcajului de timp al fişierelor;
- încărcarea mai grea a programelor;
- operarea înceată a calculatorului;
- sectoare defecte pe dischete.