

# Virusii

## •Ce este un virus de calculator?

Un virus de calculator este de obicei un program proiectat să se autoreplice și să se împrăștie, infectând cât mai multe calculatoare, fără ca utilizatorii să își dea seama de acest lucru. Virusii se împrăștie atașându-se de alte programe, fișiere EXE sau COM, iar mai recent, și documentelor WORD, EXCEL, chiar și fișierelor HLP, sau unii pot să infecteze sectorul de boot al discului. Când se lansează în execuție un fișier infectat, sau când se pornește calculatorul de pe un disc sau o dischetă virusată, se lansează și virusul în execuție. Adesea, virusul rămâne rezident în memoria calculatorului, pentru a putea infecta următorul program lansat în execuție, sau următoarea dischetă accesată.

Ceea ce fac virusii periculoși este abilitatea lor de a executa acțiuni în calculator. În timp ce unele din aceste acțiuni sunt sâcâitoare (cum ar fi afișarea unui mesaj la o anumită dată sau ca răspuns la o anumită acțiune a utilizatorului calculatorului) iar altele enervante (cum ar fi reducerea performanțelor calculatorului), există virusi care pot provoca adevărate catastrofe, distrugând fișiere de date, documente, sau făcând calculatorul inutilizabil.

Primii virusi au apărut acum câteva decenii, însă nu au cunoscut o răspândire la scară mondială decât după apariția primelor PC-uri. În 1981 firma IBM scotea pe piață, alături de gigantele mainframe-uri care îi aduseseră succesul, un calculator "personal" bazat pe noul (pe atunci) procesor produs de firma Intel, 8088. Prețul 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) și nu aveau nici un protocol de securitate inclus.

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

## •Cum se răspândesc virusii?

Virusii 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 informației între calculatoare:

Într-un studiu din 1991 al companiei Dataquest realizat la cererea National Computer Security Association din Statele Unite, cel mai des virusii se transmiteau prin dischete infectate (87 %). 43% din dischetele infectate, responsabile pentru introducerea virusilor pe calculatoarele întreprinderilor erau dischete aduse de acasă. Aproape trei sferturi (71%) din infecții au apărut în întreprinderi cu rețele de calculatoare, crescând pagubele prin rapida împrăștiere a virusilor în toată rețeaua. În mediile de rețea, riscul infectării cu virusi este mult crescut. Șapte la suta (7%) din virusi proveneau din fișiere preluate de pe diverse BBS-uri (la acea dată rețeaua Internet nu

avea răspândirea actuală). Alte surse de dischete infectate erau dischetele demo sau conținând software arhivat - circa 6% din infecțiile raportate.

- Ce pot face virușii?

Așa cum am spus și mai devreme, unii viruși sunt enervanți, iar alții pot fi deosebit de periculoși. În cazul cel mai fericit, virușii cresc dimensiunea fișierelor și reduc viteza de răspuns, afectând performanțele calculatorului dumneavoastră. Mulți viruși caută doar să se răspândească, nu să afecteze calculatorul, astfel încât nu produc daune în mod intenționat. Totuși, există posibilitatea ca și viruși benigni să interacționeze întâmplător cu alte programe sau chiar cu hardware-ul și să încetinească sau să oprească sistemul. Alți viruși sunt mult mai periculoși. Aceștia pot modifica sau distruge datele, sau pot șterge fișierele și pot reformata hard-discul.

- Care sunt simptomele unui sistem virusat?

Cei care sunt inițiați în domeniul virușilor de calculatoare nu vor avea probabil dificultăți în a spune dacă un calculator este suspect de a fi infectat cu un virus nou. Virușii se pot răspândi nestingheriți doar atâta timp cât rămân nedetecți. Din acest motiv, majoritatea virușilor nu își manifestă prezența în sistem. Numai programele antivirus pot detecta prezența unei asemenea infecții. Există, totuși, mai mulți viruși, ce își fac simțită prezența în sistem prin efectele secundare generate.

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

- fișierele sistem cresc în lungime (de exemplu în DOS 6.20 fișierul command.com are 54619 octeți, iar pe un calculator virusat el poate avea, să zicem cu 1200 de octeți mai mult, respectiv 55819);

- blocări frecvente - majoritatea virușilor sunt extrem de prost scriși și blochează calculatorul extrem de des. Virușii sunt de altfel cunoscuți ca cele mai incompatibile programe (exceptând virușii multiplatforma, ca de exemplu clasa "Concept" - virușii de .doc Word);

- mesaje ciudate, melodii sau sunete suspecte în difuzor. Mulți viruși își fac anunțata prezență 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);

- la comanda chkdisk majoritatea programelor executabile sunt raportate ca având o lungime incorectă: efect al unor viruși stealth;

- dimensiunea memoriei afișată 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 prezența unui virus;

- programele de tip self-check raportează ca au fost modificate;

- 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 înceată a calculatorului;
- sectoare defecte pe dischete.